

1 FAM 260

BUREAU OF DIPLOMATIC SECURITY (DS)

(CT:ORG-160; 07-06-2006)
(Office of Origin: DS/MGT/PPD)

1 FAM 261 ASSISTANT SECRETARY FOR DIPLOMATIC SECURITY (DS)

1 FAM 261.1 Responsibilities

(TL:ORG-128; 10-09-2003)

- a. Reports directly to the Under Secretary for Management (M).
- b. Assists the Secretary of State and the Under Secretary for Management with formulating policy on security programs worldwide for the Department and the foreign affairs community serving abroad under the authority of the chiefs of missions.
- c. Formulates and directs the implementation of diplomatic security policies to provide a secure environment for the conduct of U.S. diplomacy and the promotion of U.S. interests worldwide.
- d. Advises the Secretary and the Under Secretary for Management on diplomatic security matters and supervises the Bureau of Diplomatic Security;
- e. Establishes diplomatic security program priorities in accordance with Congressional mandates, program objectives and policies of the President, the Secretary, the Department, and the Bureau.
- f. Coordinates the provision of diplomatic security services and the exchange of security-related intelligence and operational information among the Department, foreign governments, other U.S. Government agencies, and all law enforcement authorities.
- g. Represents the Department in negotiations with other Federal agencies and foreign governments regarding diplomatic security, and counter measures program matters.
- h. Represents the Department in meetings with other countries having

mutual security concerns.

- i. Has overall substantive, and coordinating responsibility for the following Department regulatory publications:
 - (1) *Foreign Affairs Manual* Volume 1 (Organization and Functions) 1 FAM 260—Bureau of Diplomatic Security; and
 - (2) *Foreign Affairs Manual* Volume 12 (Diplomatic Security) and its related *Foreign Affairs Handbooks* in their entirety including:
 - (a) Emergency Planning Handbook (12 FAH-1);
 - (b) Protection Handbook (12 FAH-2);
 - (c) Investigations Handbook (12 FAH-3);
 - (d) Field Office Management Handbook (12 FAH-4);
 - (e) Physical Security Handbook (12 FAH-5);
 - (f) Overseas Security Policy Board (OSPB) Security Standards and Policy Handbook (12 FAH-6);
 - (g) Local Guard Program (LGP) (12 FAH-7); and
 - (h) Residential Security Program (12 FAH-8).
- j. Serves as the Director, Office of Foreign Missions (see 1 FAM 264).

1 FAM 261.2 Organization

(TL:ORG-160; 07-06-2006)

An organization chart of DS is found in 1 FAM Exhibit 261.2.

1 FAM 261.3 Authorities

(TL:ORG-128; 10-09-2003)

- a. The Bureau of Diplomatic Security within the Department of State was established pursuant to the Omnibus Diplomatic Security and Antiterrorism Act of 1986 (Public Law 99-399; 22 U.S.C. 4801, et seq). Title I of the Act defines the security functions and responsibilities of the Secretary of State. Under Delegation of Authority No. 214, the Secretary delegated these responsibilities to the Assistant Secretary for Diplomatic Security. Title II of the Act authorized the creation of the Diplomatic

Security Service, which is responsible for managing the Bureau's day to day security operations. Title III of the Act provides that the Secretary of State shall convene accountability review boards.

- b. The Overseas Security Advisory Council (OSAC) was established pursuant to the Federal Advisory Committee Act (Public Law 92-463) 5 U.S.C. App. 2, section 1 et seq. (See also 12 FAM 024.)
- c. The Omnibus Diplomatic Security and Antiterrorism Act of 1986 and Presidential Decision Directive/NSC-29 (September 16, 1994) provide authority for the Overseas Security Policy Board (OSPB).
- d. The legal authorities for the Freedom of Information and Privacy Act Program within DS (12 FAM) are:
 - (1) The Freedom of Information Act (FOIA) (Public Law 89-487), as amended, 5 U.S.C. 552;
 - (2) The Privacy Act of 1974, 5 U.S.C. 552a (Public Law 93-579), as amended; and
 - (3) Executive Order (E.O.) 12958 (classified national security information).
- e. Section 36 of the State Department Basic Authorities Act of 1956 (Public Law 84-885), as amended (22 U.S.C. 2708, provides authority for the counter terrorism rewards program.
- f. Section 102 of Public Law 105-323 (1998) provides authority for the war criminals rewards program.
- g. Section 37 of the State Department Basic Authorities Act of 1956 (22 U.S.C. 2709) provides authority for certain responsibilities of Diplomatic Security special agents (i.e., passport and visa fraud, investigations, protection).
- h. Section 160 of the Foreign Relations Authorization Act, Fiscal Years 1988 and 1989 (Public Law 100-204), as amended, provides authority for construction security certifications.
- i. Section 103 (a)(2)(G) of the Omnibus Diplomatic Security and Antiterrorism Act of 1986 and Part II of the Foreign Assistance Act of 1961 (Public Law 87-195), as amended (22 U.S.C. 2349aa), provide authority for the antiterrorism assistance program.
- j. Under the Foreign Missions Act of 1982 (as codified at 22 U.S.C. 4314), and 3 U.S.C. 202 (8), 202 (10), and 208, the Department of State

provides for the extraordinary protection of foreign missions and officials, international organizations and foreign dignitaries under certain circumstances throughout the United States. (See also Executive Order 12478 (1984) and Delegation of Authority No. 214, Section 8 (1994).)

- k. The Bureau of Diplomatic Security has authority to conduct personnel security and suitability investigations based on the following executive orders and laws:
 - (1) Section 103 (a)(2)(B), Omnibus Diplomatic Security and Terrorism Act of 1986 (22 U.S.C. 4802(a)(2)(B));
 - (2) E.O. 10450 dated April 27, 1953; and
 - (3) E.O. 12968 dated August 2, 1995.
- l. Public Law 89-554 (5 U.S.C. 7531 - 7533), enacted September 6, 1966, gives to the heads of major U.S. Government agencies, including the Secretary of State, the power to summarily suspend and remove any employee of the agency when deemed necessary "in the interests of national security." codified The Department's basic authorizing legislation for its personnel security program is codified in 5 U.S.C. 7531 - 7533.
- m. The legal authorities for the Office of Foreign Missions are set forth in 1 FAM 264.1.
- n. Other authorities, as appropriate.

1 FAM 261.4 Public Affairs

(CT:ORG-133; 08-03-2004)

The Public Affairs staff, under the direct supervision of the Assistant Secretary for Diplomatic Security:

- (1) Advises the Assistant Secretary for Diplomatic Security on media relations and outreach efforts;
- (2) Formulates DS press guidance for the Secretary's spokesperson and responds to all media inquiries regarding DS and security measures at the Department;
- (3) Formulates and conducts an outreach program to inform the public and constituent audiences about the Bureau's activities;
- (4) Coordinates production of all DS media, including managing the DS public web site; and

- (5) Develops and disseminates materials to the public, the media, and Department personnel on the Department's security programs and DS activities.

1 FAM 262 DEPUTY ASSISTANT SECRETARY FOR DIPLOMATIC SECURITY AND DIRECTOR OF THE DIPLOMATIC SECURITY SERVICE (DS/DSS)

(TL:ORG-89; 08-28-2000)

- a. Advises the Assistant Secretary for Diplomatic Security on the formulation and implementation of security programs and policies for the Department of State and the foreign affairs community.
- b. Serves as the Director of the Diplomatic Security Service (DSS) and manages the day-to-day operations of the Department's security program at U.S. diplomatic and consular missions abroad.
- c. Chairs the Overseas Security Policy Board (OSPB), whose members include the security directors of the foreign affairs and intelligence agencies represented at Foreign Service posts abroad.
- d. Directs personal protective services for the Secretary of State, other Department officials, certain resident foreign dignitaries and dignitaries on official visits to the United States.
- e. Oversees the worldwide law enforcement and protective security responsibilities of the Diplomatic Security Service.
- f. Oversees the Department's personnel security program, which determines the issuance and maintenance of employee security clearances.
- g. Supervises the DSS Legal Counsel, who provides legal support to the Bureau in legislative, regulatory, and procedural matters, in coordination with the Office of the Legal Adviser (L).
- h. Chairs the Secretary's Overseas Security Advisory Council (OSAC), which promotes cooperation between U.S. business and private sector interests abroad and the Department's security programs.
- i. Provides direct management oversight to the following DSS Offices:

- (1) Overseas Operations (DS/DSS/OP);
- (2) Protection (DS/DSS/P);
- (3) Investigations and Counterintelligence (DS/DSS/ICI);
- (4) Intelligence and Threat Analysis (DS/DSS/ITA);
- (5) Field Office Management (DS/DSS/FLD);
- (6) Overseas Security Advisory Council (DS/DSS/OSAC); and
- (7) Office of Antiterrorism Assistance (DS/DSS/ATA).

1 FAM 262.1 The Overseas Security Advisory Council (DS/DSS/OSAC)

(TL:ORG-89; 08-28-2000)

- a. Establishes continuing liaison and provides for operational security cooperation between State Department security functions and the private sector.
- b. Provides for regular and timely interchange of information between the U.S. private sector and the Department concerning developments in the security environment abroad.
- c. Recommends methods and provides material for coordinating security planning and implementation of security programs.
- d. Recommends methods to protect the competitiveness of U.S. businesses operating worldwide.

1 FAM 262.2 Assistant Director for International Programs (DS/DSS/IP)

(CT:ORG-144; 11-14-2005)

- a. Serves as the focal point within the Bureau of Diplomatic Security (DS) for coordinating international security programs.
- b. Manages and directs the formulation, planning, coordination, policy development and implementation of security programs that protect our U.S. missions abroad from physical, electronic, and chemical/biological attack.

1 FAM 262.2-1 Office of Regional Directors (DS/IP/RD)

(CT:ORG-144; 11-14-2005)

- a. DS/IP/RD is divided by geographic region into five Directorates, each headed by a Regional Director. The Regional Directors are the primary liaison between DS and the Department's Regional Bureau Executive Directors, Post Management Officers and Desk Officers.
- b. The Regional Directorates are:
 - (1) Africa Region (DS/RD/AF);
 - (2) Western Hemispheric Region (DS/RD/WHA);
 - (3) East Asia and Pacific Region (DS/RD/EAP);
 - (4) European Region (DS/RD/EUR);and
 - (5) Near Eastern and South Asian Region (DS/RD/NEA).
- c. Each Regional Director:
 - (1) Serves as the primary point of contact within the Department and other U.S. Government agencies on security programs and activities at U.S. missions abroad.
 - (2) Ensures that DS security programs and activities at posts abroad are responsive, effective, and conform with Department policy, regulations and procedures.
 - (3) Establishes priorities for all security programs abroad and coordinates the planning and review of security services at posts abroad.
 - (4) Provides technical assistance to posts abroad. Reviews and monitors post progress on individual security projects and programs.
 - (5) Coordinates all briefing papers and related materials concerning security programs abroad for DS and senior Department management.

1 FAM 262.2-2 Office of Special Programs and Coordination (DS/IP/SPC)

(CT:ORG-144; 11-14-2005)

- a. Coordinates the Marine Security Guard Program, Special Programs,

Weapons of Mass Destruction Program and Emergency Plans for U.S. missions abroad.

- b. Serves as contact with the military liaison for planning and force protection detachments/operations.
- c. Provides representation and expertise in response to crisis situations, including Department task forces and security support teams.

1 FAM 262.2-2(A) Marine Security Guard Staff (DS/SPC/MSG)

(CT:ORG-144; 11-14-2005)

- a. Manages the Marine Security Guard (MSG) Program for the Department.
- b. Maintains liaison with the Commanding Officer and/or staff of the MSG Battalion and the Security Division, Homeland Defense Branch, Headquarters, U.S. Marine Corps.

1 FAM 262.2-2(B) Special Programs and Plans Division (DS/SPC/SPP)

(CT:ORG-144; 11-14-2005)

- a. Provides liaison to the Department of Defense Regional Combatant Commands.
- b. Manages the following staffs.
 - (1) Emergency Planning Staff
 - (a) Maintains the 12 FAH-1 Emergency Planning Handbook, the principle source of guidance for posts to produce Emergency Action Plans (EAPs). Provides supporting emergency planning guidance as necessary.
 - (b) Reviews completed EAPs submitted by posts. Work with posts to make required changes or suggested improvements. Approve and publish EAPs as appropriate.

(2) Special Operations Staff

Coordinates the Department of Defense Special Operations units to assist missions in preparing for or responding to crises and other requirements.

1 FAM 262.2-2(C) Weapons of Mass Destruction Division (DS/SPC/WMD)

(CT:ORG-144; 11-14-2005)

- a. Responsible for providing weapons of mass destruction (WMD) countermeasures training and equipment to personnel under the authority of a chief of mission to aid in surviving a chemical, biological, radiological, or nuclear attack.
- b. Provides additional training and equipment overseas to First Responders (volunteers approved at post for such service), Local Guards, Bodyguards, Surveillance Detection Personnel, and other designated security personnel.
- c. In addition to the overseas training, DS/SPC/WMD provides:
 - (1) Domestic First Responder and other WMD related training for personnel scheduled for overseas assignment;
 - (2) Escape mask training and equipment for Department employees assigned to designated State Department domestic facilities;
 - (3) Training to domestic Department Emergency Response Teams; and
 - (4) Other WMD awareness and countermeasures training.
- d. Researches and tests new WMD countermeasures equipment to ensure the equipment meets new or changing needs. Plans procurements for deployment to Department facilities overseas and domestically.

1 FAM 262.2-3 Office of Intelligence and Threat Analysis (DS/IP/ITA)

(CT:ORG-144; 11-14-2005)

- a. Acts as the interface between DS and the U.S. intelligence community to ensure that timely intelligence information is made available to DS bureau decision makers and DS officers in the field. Initiates and issues threat notifications to the field.
- b. Researches, monitors, and analyzes all source intelligence on terrorist activities and threats directed against U.S. citizens and U.S. diplomatic and consular facilities abroad, as well as threats against the Secretary of State, senior U.S. officials, visiting foreign dignitaries, resident foreign diplomats, and foreign missions in the United States, for whom DS has protective security responsibility.

- c. Provides real time threat assessments in support of operational and policy decision-making by senior DS and Department officials.
- d. Revises the Department's Security Environment Threat List (SETL) on a semi-annual basis.
- e. DS/IP/ITA is divided into three geographic regions, each headed by a Division Chief. The regions are:
 - (1) Near Eastern & European Division (DS/ITA/NEA-EUR);
 - (2) Western Hemisphere Division (DS/ITA/WHA); and Surveillance and Tactical Analysis Branch:
 - (3) Africa, South & East Asia and Pacific Division (DS/ITA/AF-SA-EAP).

1 FAM 262.2-4 Office of Overseas Protective Operations (DS/IP/OPO)

(CT:ORG-144; 11-14-2005)

- a. Directs the development of standards, policies and procedures associated with local guard, residential security, surveillance detection and high threat protection programs at U.S. missions abroad.
- b. Directs the implementation of facility programs and ensures that local guard and residential security standards are met to protect diplomatic personnel, facilities and residences abroad.
- c. Directs the conduct of Program Management Reviews to evaluate posts management of local guard, residential security and surveillance detection programs.

1 FAM 262.2-4(A) Facility Protection Division (DS/OPO/FPD)

(CT:ORG-144; 11-14-2005)

- a. Develops security policies and standards for protecting personnel, residences, and facilities under the authority of a chief of mission.
- b. Provides for local guard, residential security and surveillance detection requirements to protect personnel, residences, and facilities under the authority of a chief of mission.
- c. Maintains liaison with other foreign affairs and intelligence community

agencies on local guard, residential security and surveillance detection program matters.

- d. Conducts Program Management Reviews of posts local guard, residential security and surveillance detection programs. Make recommendations to enhance the programs and track compliance.

1 FAM 262.2-4(B) Operational Support Division (DS/OPO/OSD)

(CT:ORG-144; 11-14-2005)

- a. Develops and implements policies and procedures to ensure local guard contracts are awarded in a timely manner.
- b. Provides guidance and support in preparing contract solicitations, modifications and the conduct of technical evaluation panels.
- c. Directs the processing and certification for invoice payments submitted by contractors providing services for the High Threat Protection Division.
- d. Develops and implements policies and procedures to ensure local guard, residential security and surveillance detection field budget plans are submitted by posts in a timely manner.

1 FAM 262.2-4(C) High Threat Protection Division (DS/OPO/HTP)

(CT:ORG-144; 11-14-2005)

- a. Develops security policies and standards to manage and provide for protective security details at high threat missions abroad.
- b. Directs the administration and operations of the contractor-provided security personnel to ensure protection provided by Protective Security Specialists (PSSs) is of the highest caliber.
- c. Coordinates with DS program offices, RSOs, and military liaisons to ensure current operations are sufficiently supported in logistical and operational matters.

1 FAM 262.3 Assistant Director for Training (DS/DSS/T)

(CT:ORG-146; 11-23-2005)

- a. Advises the Deputy Assistant Secretary and Director of the Diplomatic Security Service on the formulation and implementation of all Training programs and policies for the Bureau of Diplomatic Security.
- b. Serves as the Assistant Director for Training with a directorate comprised of the Office of Antiterrorism Assistance; the Office of Training and Performance Support; and the Office of Mobile Security Training.
- c. Oversees the development, training, and coordination of related equipment and assistance to foreign government security and law enforcement personnel to deter and counter terrorism.
- d. Directs the development and implementation of training courses to provide specialized training in technical security.
- e. Directs the formulation, coordination, and implementation of training programs that promote the professional development of Diplomatic Security (DS) personnel.
- f. Oversees the specialized training at Foreign Service (FS) posts on security topics on a regular and emergency basis and provides emergency security support to posts abroad during periods of high threat, crisis or natural disaster.

1 FAM 262.3-1 Office of the Antiterrorism Assistance Program (DS/T/ATA)

(CT:ORG-160; 07-06-2006)

- a. Provides training and related equipment and assistance to foreign government security and law enforcement personnel to deter and counter terrorism.*
- b. Develops training programs in coordination with selected U.S. mission country teams and host governments that provide an efficient and effective means of deterring and countering terrorism through modern and humane techniques and practices.*
- c. Coordinates training and assistance with the Office of the Coordinator for Counterterrorism (S/CT), the Bureau of Democracy, Human Rights, and Labor (DRL), other agencies, departments, and organizations.*

1 FAM 262.3-2 Office of Training and Performance Support (DS/T/TPS)

(CT:ORG-146; 11-23-2005)

- a. Formulates, coordinates, and implements programs that promote the training and professional development of Diplomatic Security (DS) personnel.
- b. Provides specialized security training for other employees of the Department and foreign affairs agencies and their eligible family members.
- c. Assists in training other local, state, and Federal law enforcement personnel.
- d. Provides analysis, design, development, and evaluation to support standardization and accreditation of applicable DS training programs.
- e. Provides leadership and management initiatives, training newsletters, and professional video services to augment existing training programs and expand the professional development opportunities available to DS employees.
- f. Provides a full range of administrative support services to include procurement actions, audiovisual services, budgeting, external training, preparing the DS Training Catalog, maintaining student-training records, registrar services, and building maintenance oversight.

1 FAM 262.3-2(A) Security and Law Enforcement Training Division (DS/T/TPS/SLTD)

(CT:ORG-146; 11-23-2005)

- a. Develops courses and provides instruction and course coordination for:
 - (1) Basic Special Agent training;
 - (2) Basic Regional Security Officer training;
 - (3) Special Agent In-Service training; and
 - (4) Regional Security Officer In-Service training.
- b. Develops specialized training courses and provides instruction of these courses to DS and other personnel to meet DS' global mission requirements.

- c. Provides subject matter expertise for the Security Overseas Seminar to include briefings on surveillance detection and explosives recognition.
- d. Provides specific security training to chiefs of mission, DCMs, principal officers, post security officers, and foreign service national (FSN) investigators.
- e. Provides specialized training in security subjects, such as weapons, defensive tactics/room entry, counter-terrorist driving, surveillance detection, and improvised explosive device handling.

1 FAM 262.3-2(A)(i) Overseas Training Branch (DS/SLTD/OTB)

(CT:ORG-146; 11-23-2005)

- a. Develops courses and provides instruction and course coordination for:
 - (1) Basic Regional Security Officer training; and
 - (2) Regional Security Officer In-Service training.
- b. Provides subject matter expertise for the Security Overseas Seminar and SAFE to include briefings on surveillance detection and explosives recognition.
- c. Provides specific security training to chiefs of mission, DCMs, principal officers, post security officers, foreign service national (FSN) investigators, and Marine security guards.

1 FAM 262.3-2(A)(ii) Domestic Training Branch (DS/SLTD/DTB)

(CT:ORG-146; 11-23-2005)

- a. Develops courses and provides instruction and course coordination for:
 - (1) Basic Special Agent training; and
 - (2) Special Agent In-Service training.
- b. Develops specialized training courses and provides instruction of these courses to DS and other personnel to meet DS' global mission requirements to include high threat protection training.
- c. Supports as a Partner Organization (PO) the Federal Law Enforcement Training Center (FLETC).

1 FAM 262.3-2(A)(iii) Special Skills Training Branch (DS/SLTD/SSB)

(CT:ORG-146; 11-23-2005)

- a. Develops courses and provides instruction and course coordination for:
 - (1) All standardized DS firearms training and qualification to include the standard DS issued personal and support weapons and special weapons as approved by the Firearms Policy Review Board.
 - (2) All standardized DS training in Defensive Tactics and Room Entry Tactics in support of Special Agents' responsibilities to conduct law enforcement activities and protective security operations.
 - (3) All standardized DS Security Driver Training programs in support of Special Agents' responsibilities to conduct law enforcement activities and protective security operations.
 - (4) All standardized DS Explosive Countermeasures Training in support of the DS security mission to include courses such as Introduction to Explosives and IEDs, Building and Vehicle Searches, X-ray Interpretation, and Post Blast Investigations, etc.
- b. Provides subject matter expertise to the Firearms Policy Review Board and all DS Directorates relative to standardized tactics and operations for firearms, defensive tactics, room entry tactics, security driver tactics, and explosive countermeasures.

1 FAM 262.3-2(B) Security Engineering and Computer Security Training Division (DS/T/TPS/SECD)

(CT:ORG-146; 11-23-2005)

- a. Develops training for technical security and information assurance topics to include technical surveillance countermeasures, technical security systems, and information system security.
- b. Presents training and briefings to diverse groups to include chiefs of mission, deputy chiefs of mission, foreign service personnel, civil service personnel, security specialists, security officers, U.S. Navy Seabees, U.S. Marines, cleared American guards, construction surveillance technicians, and others throughout the U.S. government.
- c. Manages, coordinates and administers all fundamental and advanced technical surveillance countermeasures and technical security training programs for:

- (1) Security Engineering Officers;
 - (2) Security Technical Specialists;
 - (3) U.S. Navy Seabees;
 - (4) Construction Surveillance Technicians;
 - (5) Cleared American Guards; and
 - (6) Site Security Managers.
- d. Manages, coordinates, and administers information assurance training programs in compliance with the Federal Information Security Management Act.
 - e. Serves as the principal technical security training representative of the Department of State to other federal agencies and groups.

1 FAM 262.3-3 Office of Mobile Security Deployments (DS/T/MSD)

(CT:ORG-146; 11-23-2005)

- a. Provides emergency security support to posts abroad during periods of high threat, crisis or natural disaster.
- b. Assists DS protective details with tactical support, both domestically and abroad, in high threat situations.
- c. Provides specialized training at Foreign Service posts on a variety of security topics, as directed.

1 FAM 262.4 Assistant Director for Domestic Operations (DS/DSS/DO)

(CT:ORG-160; 07-06-2006)

Under Development.

1 FAM 262.4-1 Office of Investigations and Counterintelligence (DS/DO/ICI)

(CT:ORG-160; 07-06-2006)

- a. Oversees the development and direction of a wide range of investigative*

programs and activities, including:

- (1) Passport and visa issuance and use;*
- (2) Protective intelligence;*
- (3) Counterintelligence;*
- (4) Personnel security and suitability;*
- (5) Investigations and security assistance to other U.S. Government agencies;*
- (6) Liaison with INTERPOL;*
- (7) Counterterrorism rewards and war criminal rewards programs; and*
- (8) Other special investigations.*

b. Oversees and directs the operation of all domestic Diplomatic Security Field and Resident Agent Offices.

c. DS Field and Resident Agent Offices:

- (1) Perform criminal investigations of passport and visa issuance and/or use crimes and protective intelligence investigations.*
- (2) Conduct background security investigations of prospective and incumbent employees of the Department of State and other agencies, as requested.*
- (3) Protect foreign dignitaries and resident foreign officials.*
- (4) Provide protective and security related liaison with foreign diplomatic and consular missions located in the geographic region of the field offices.*
- (5) Perform liaison functions with local and Federal law enforcement agencies for the purpose of information and intelligence sharing.*
- (6) Facilitate investigative efforts of the Office of Inspector General (OIG), as referred by DS headquarters.*

1 FAM 262.4-1(A) Criminal Investigations Division (DS/ICI/CR)

(CT:ORG-160; 07-06-2006)

- a. Coordinates investigative complaints, allegations, information, and unusual incidents involving Department of State employees and all U.S. Government personnel under the authority of a chief of mission.*
- b. Responsible for the administrative and operational case control of crimes associated with passport and visa issuance and use.*
- c. Responsible for administrative and operational case control of non-routine criminal investigations, as authorized by law and regulations.*
- d. Coordinates with other Federal, state, and local law enforcement entities when it appears that violations of law or regulations have occurred for which they have investigative authority.*
- e. Conducts and/or coordinates:*
 - (1) Criminal investigation leads for other Federal, state, and local agencies, as requested;*
 - (2) Criminal investigations leads on U.S. Government personnel under authority of the chief of mission;*
 - (3) Physical security investigations;*
 - (4) Special criminal investigations and inquiries; and*
 - (5) Investigations referred by the Office of Inspector General.*

1 FAM 262.4-1(B) Protective Intelligence Investigations Division (DS/ICI/PII)

(CT:ORG-160; 07-06-2006)

- a. Directs, coordinates, and conducts protective intelligence investigations involving terrorist threats and/or hostile activities directed against all U.S. Government personnel, facilities, and interests abroad under the authority of the chief of mission.*
- b. Conducts investigations into terrorist threats or other hostile activity directed against the Secretary of State, other Department of State personnel and facilities, and foreign dignitaries and facilities in the United*

States.

- c. Provides protective intelligence operational support for the Secretary of State, certain high threat and/or high profile visiting foreign dignitaries, and others, as directed.*
- d. Administers the Department of State's counterterrorism rewards and war criminal rewards programs (see 2 FAM 940).*
- e. Coordinates foreign government requests for investigative and/or forensic assistance from the U.S. Government to assist foreign governments in the resolution of serious incidents such as bombings or assassination attempts.*
- f. Administers DS participation in the Department of Justice Joint Terrorism Task Force Programs.*

1 FAM 262.4-1(C) Counterintelligence Division (DS/ICI/CI)

(CT:ORG-160; 07-06-2006)

- a. Develops and directs the Department's worldwide defensive counterintelligence program.*
- b. Monitors, identifies, and neutralizes foreign intelligence efforts directed against Department of State and U.S. mission facilities and personnel.*
- c. Conducts substantive counterintelligence investigations and inquiries of:*
 - (1) Allegations of espionage;*
 - (2) Technical penetration of U.S. missions abroad;*
 - (3) Developmental targeting;*
 - (4) Recruitment and recruitment attempts by foreign intelligence services;*
 - (5) Exploitable conduct of U.S. Government employees;*
 - (6) Suspect activities involving Foreign Service nationals (FSN); and*
 - (7) Other matters relevant to counterintelligence.*
- d. Conducts security screening of Department personnel and contractors who are assigned to designated critical intelligence threat post countries.*

1 FAM 262.4-1(D) Professional Responsibility Division (DS/ICI/PR)

(CT:ORG-160; 07-06-2006)

a. Conducts investigations which may include:

- (1) Unauthorized disclosure of classified or other sensitive information;*
- (2) Substance abuse;*
- (3) Financial misconduct;*
- (4) Discharge of a firearm;*
- (5) Loss of credentials and/or identification pins and/or special protective equipment;*
- (6) Abuse of diplomatic pouch;*
- (7) Missing employees;*
- (8) Sexual misconduct (only in cases where such conduct has the potential to be prejudicial to the U.S. Government, make the employee vulnerable to coercion or place the employee or others in physical danger);*
- (9) Spousal abuse involving employee assigned abroad; and*
- (10) Other cases involving employee suitability.*

b. Conducts and coordinates:

- (1) Special criminal investigations and inquiries; and*
- (2) Investigations referred by the Office of Inspector General (OIG).*

1 FAM 262.4-2 Office of Domestic Facilities Protection (DS/DO/DFP)

(CT:ORG-160; 07-06-2006)

a. Manages the physical security and security support programs for all Department domestic facilities;

b. Responsible for the protection of personnel, information, and property at all Department domestic facilities.

- c. Directs the Uniformed Protection and Security Support Divisions.*
- d. Represents the Department on the Interagency Security Committee, and other applicable interagency groups for domestic security.*
- e. Serves as the Department's primary point of contact for Federal, state, local government, and law enforcement agencies related to domestic facility security and protection matters.*
- f. Develops and implements domestic security standards, policies, and guidelines.*
- g. Coordinates all domestic security delegations of authority with the General Services Administration, Department of Homeland Security/Federal Protective Service or other entities as appropriate.*

1 FAM 262.4-2(A) Uniformed Protection Division (DS/DFP/UPD)

(CT:ORG-160; 07-06-2006)

- a. Manages the uniformed protective services guard contracts and oversees guard services at all Department domestic facilities.*
- b. Manages and operates the domestic Security Control Center.*
- c. Manages uniformed security officers for the Diplomatic Security Service's (DSS) protective operations.*
- d. Provides access and property control at domestic facilities.*
- e. Provides domestic site security for the Department's Secretariat.*
- f. Coordinates and determines security needs for all domestic classified and unclassified conferences, special events, or special access.*
- g. Provides security and operational oversight for large scale domestic Special Events.*
- h. Provides security oversight for domestic Facility Emergency Action Plans and input to all domestic Occupant Emergency Plans.*
- i. Manages or coordinates the appropriate response to security related emergency situations (e.g., fires, bomb threats, suspicious packages, and security alarms) in all domestic Department facilities.*

1 FAM 262.4-2(B) Security Support Division (DS/DFP/SSD)

(CT:ORG-160; 07-06-2006)

- a. Responsible for Building Pass Identification Issuance, Security Systems Administration, Domestic Security Officer's Program, DFP budget, policy, and procedural development and implementation.*
- b. Manages the DSS Identification Media Program, which develops and issues ID cards, DSS credentials, badges, and security pins.*
- c. Manages the Diplomatic Security Identification Service (DSIS) Program, which develops and issues all DOS Building Pass Identification Cards (BPIC) in compliance with Federal Information Processing Standard Publication (FIPS PUB) 201 standards and associated Special Publications.*
- d. Provides customer support for building pass ID media and alarm system operations.*
- e. Provides security briefings for procedural security requirements, security awareness, and violence in the workplace.*
- f. Provides access history for employee or visitor ingress and egress to internal or external law enforcement and other authorized entities.*
- g. Manages the Intelligence Community Badge Program in coordination with the Bureau of Intelligence and Research (INR).*
- h. Provides employee training for the operation of access control systems/media and alarm systems.*
- i. Manages the domestic Lock and Key Program, which maintains inventories and authorizes issuance of all security keys and locks in coordination with other DS Offices, the Bureau of Administration(A) , and the Department's Lock Contractor.*
- j. Offers a crime prevention program for all Department employees.*
- k. Coordinates theft investigations with the Office of Inspector General (OIG) or other law enforcement organizations, as appropriate.*

1 FAM 262.4-3 Office of Protection (DS/DO/P)

(CT:ORG-160; 07-06-2006)

- a. Manages and directs protective security for the Secretary of State, other*

official representatives of the United States and foreign governments, and Department protective liaison programs.

- b. Manages and coordinates the protection of certain foreign missions and officials in the United States.*
- c. Administers reimbursements to Federal, state and local law enforcement agencies or private security companies for expenses incurred in the protection of certain foreign government and United Nations missions and officials.*

1 FAM 262.4-3(A) Dignitary Protection Division (DS/P/DP)

(CT:ORG-160; 07-06-2006)

- a. Coordinates protective services to visiting foreign dignitaries, resident foreign officials, and U.S. Government officials.*
- b. Organizes and manages protective services for special events involving multiple protectees.*
- c. Coordinates with the U.S. Secret Service and other Federal, state, and local law enforcement agencies or private security companies involved with protective security.*

1 FAM 262.4-3(B) Protective Liaison Division (DS/P/PL)

(CT:ORG-160; 07-06-2006)

- a. Maintains liaison with appropriate U.S. Government agencies, foreign governments, Federal, state and local law enforcement agencies, or private security companies assisting the Department with protective security.*
- b. Coordinates and monitors state and local police protection for certain foreign missions.*
- c. Provides information and assists foreign missions with security threats. Offers guidance on the security aspects of diplomatic and consular immunity.*
- d. Administers the reimbursement of funds to Federal, state, and local law enforcement agencies or private security companies which provide extraordinary protective services to certain resident foreign officials, facilities, and visiting foreign government officials.*

1 FAM 262.4-3(C) Secretary's Detail (DS/P/SD)

(CT:ORG-160; 07-05-2006)

Provides protection for the Secretary of State and immediate family and comprehensive security coverage of the Secretary's residence.

1 FAM 262.5 Diplomatic Security Command Center (DS/DSS/CC)

(CT:ORG-160; 07-06-2006)

The Diplomatic Security Command Center (DS/DSS/CC), under the direct supervision of the Director for Diplomatic Security provides the following 24/7 services:

- (1) Manages and collates incoming overseas security-related information regarding threats, security incidents, and unfolding emergency situations and disseminates that information appropriately and rapidly to DS and Department leadership;*
- (2) Coordinates threat and security-related information with the Department's Operations Center;*
- (3) Disseminates guidance and important information to the field from the DS leadership;*
- (4) Serves as support and point of contact (POC) for all after-hours calls for DS field offices, Regional Security Offices (RSO) and Security Engineering Offices (SEO);*
- (5) Monitors after-hours police liaison issues for the DS bureau and OFM, to include law enforcement response to incidents involving foreign dignitaries and resident foreign diplomats;*
- (6) Monitors the Blue Force Tracker – the GPS-based 911 tracking and call-for-help system used by high and critical-threat protective details—and makes appropriate rapid notifications when an activation occurs;*
- (7) Serves as the main point of contact for all DS protective security details, to include monitoring of radio frequencies;*
- (8) Serves as DS's after-hours point of contact for the National Counterterrorism Center on emerging threats and significant surveillance incidents;*

- (9) *Performs urgent Treasury Enforcement Communications System (TECS) and National Crime Information Center (NCIC) queries for RSOs and special agents in the field and maintains all DS warrant information;*
- (10) *Produces the DS Overnight Update, and coordinates and disseminates all spot reports;*
- (11) *Establishes DS-specific task forces at the discretion of DS leadership;*
- (12) *Coordinates DS's participation in daily-interagency Secure Voice Teleconferencing;*
- (13) *Assembles information on a daily basis regarding security incidents, threats, and surveillance activity from overseas and publishes the "Diplomatic Security Daily" publication, which is disseminated throughout the security and intelligence community daily;*
- (14) *Monitors remotely, through the newly created Technical Operations Group (TOG), overseas Lock and Leave posts' technical security systems (intrusion detection, automated access control, CCTV systems, and imminent danger notifications systems) and makes appropriate notifications within DS and at the affected post; and*
- (15) *Provides an embedded DSCC Watch Officer at the Department of Homeland Security (DHS) Operation's Center to share information between DHS and DS.*

1 FAM 263 DEPUTY ASSISTANT SECRETARY AND ASSISTANT DIRECTOR FOR COUNTERMEASURES(DS/C)

(CT:ORG-160; 07-06-2006)

- a. Manages all security countermeasures and information security programs and reports to the Assistant Secretary for Diplomatic Security.
- b. Directs and provides management oversight to the Offices of:
 - (1) Office of Physical Security Programs (DS/C/PSP);
 - (2) Office of Security Technology (DS/C/ST); and
 - (3) Office of Domestic Operations (DS/C/DO).

- c. Formulates security policy and program plans for countermeasures, physical security, domestic operations, and security technology programs.
- d. Represents the Department in negotiations with other Federal agencies on security issues regarding countermeasures, physical security, and security technology.
- e. Chairs the interagency Technical Security Coordinating Group (TSCG).
- f. Represents the Department on the executive committees of the National Security Telecommunications and Information System Security Committee (NSTISSC).

1 FAM 263.1 Office of Physical Security Programs (DS/C/PSP)

(TL:ORG-142; 09-28-2005)

- a. Directs and assists in the development of standards, policies and procedures for protecting personnel, facilities, and the national security information of the Department and foreign affairs agencies abroad.
- b. Directs the implementation of the physical security programs and ensures that the Overseas Security Policy Board (OSPB) physical security standards are met to protect diplomatic personnel, facilities, and on-compound housing abroad.
- c. Develops and directs the implementation of the requirements of the Secure Embassy Construction and Counterterrorism Act of 1999 mandating setback and collocation of U.S. mission facilities abroad. Provides annual report to Congress on waivers granted by the Secretary and the Assistant Secretary for Diplomatic Security.
- d. Develops and implements policies and procedures on certifying to Congress that appropriate action has been taken to protect all new office building construction and major renovation projects intended for the storage of classified materials or the conduct of classified activities.
- e. Develops and directs the implementation of the construction security program to ensure that construction and other materials destined for controlled access areas at post facilities abroad are protected from acquisition to installation.
- f. Directs the implementation of DS' Research and Development Program to identify protective measures against terrorism.

- g. Directs the implementation of the Defensive Equipment and Armored Vehicle Programs to ensure post requirements for defensive and special equipment and armored vehicles are met.
- h. Directs and develops domestic guidelines, policies and procedures for protecting Department personnel, facilities, and national security information throughout the United States.
- i. Directs the implementation of the domestic physical security programs and ensures that regulatory requirements are met to protect Department facilities, personnel, and classified operations throughout the United States.

1 FAM 263.1-1 Physical Security Division (DS/PSP/PSD)

(TL:ORG-142; 09-28-2005)

- a. Provides oversight to Overseas Buildings Operations (OBO) new office building (NOB) construction major renovation projects and ensures compliance with OSPB security standards.
- b. Evaluates NOB construction and major renovation projects and ensures the proper application of physical security and other standards in the selection, design, construction, and modification of buildings abroad to be occupied by the Department and foreign affairs agencies.
- c. Certifies physical security equipment to meet specified performance criteria through in-house and independent testing.
- d. Manages the development and installation of secure transit systems.
- e. Performs technical security countermeasures and physical security standards compliance inspections of new office buildings under construction by the Department and prepares Congressional certifications with respect to the suitability of new U.S. embassies and consulates for classified operations and protection of personnel.
- f. Manages DS' Research and Development Program that evaluates and recommends physical security countermeasures against the terrorism threat.

1 FAM 263.1-1(A) Project Coordination Branch (DS/PSD/PCB)

(TL:ORG-142; 09-28-2005)

- a. Provides project managers and/or coordinators for physical security renovations or modifications to existing Department facilities abroad.
- b. Provides project evaluation to ensure proper application of physical security standards in the selection, design, construction, and modification of overseas buildings to be occupied by the Department and foreign affairs agencies.
- c. Coordinates all collocation and setback requirements of the Secure Embassy Construction and Counterterrorism Act of 1999 for all newly acquired facilities.
- d. Coordinates and responds to requests from Congress, the Inspector General, Department offices, and other agencies for information or guidance.
- e. Coordinates with OBO, members of the OSPB, and the intelligence community to ensure compliance with OSPB physical security standards.

1 FAM 263.1-1(B) New Office Building Branch (DS/PSD/NOB)

(TL:ORG-142; 09-28-2005)

- a. Provides project oversight to ensure that OSPB security standards and SECCA requirements are implemented for NOBs abroad. Performs liaison/coordination functions for NOBs with OBO, the relevant diplomatic post, and other DS elements. This effort entails actively tracking projects from the initial planning phase through final accreditation and move-in.
- b. Key participant in site selection surveys for all New Embassy Compounds (NEC).
- c. Reviews all OBO project/design development plans for new construction.
- d. Coordinates with the Intelligence Community to ensure technical, political violence, and terrorism threat security standards are met.
- e. Certifies physical security equipment, (such as doors and barriers) that meet specified performance criteria, (e.g. ballistic resistance, forced

entry, and anti-ram) through in-house and independent testing.

1 FAM 263.1-1(C) Certification, Accreditation, Transit Security Branch (DS/PSD/CAT)

(TL:ORG-142; 09-28-2005)

- a. Recommends and implements construction security policies abroad.
- b. Determines the appropriate level of construction security coverage abroad in accordance with the OSPB construction security standards for all NOBs and major renovation/rehabilitation projects.
- c. Recommends and implements policies and procedures for the certification of all such projects abroad in accordance with Section 160(a) of the Foreign Relations Authorization Act, Fiscal Years 1988 and 1989 (Public Law 100-204), enacted December 22, 1987, as amended by Section 135 of the Foreign Relations Authorizations Act, Fiscal Years 1990 and 1991 (Public Law 101-246), enacted February 16, 1990.
- d. Recommends policies and develops procedures to ensure that construction and other materials destined for installation abroad are provided the necessary protection from the time of acquisition until installation.
- e. Promotes the development of state-of-the-art secure transit systems and installation of the approved systems.
- f. Conducts accreditation inspections of projects certified to Congress to ensure compliance with OSPB security standards, conformity with Construction Security Plans, and proper operation of the security systems. Accreditation is required prior to occupancy of a facility and the processing and storage of classified information in the facility.
- g. Coordinates inspections programs, schedules, and objectives with the OBO and other appropriate U.S. Government agencies.

1 FAM 263.1-2 Facilities Security Division (DS/PSP/FSD)

(TL:ORG-142; 09-28-2005)

- a. Directs, manages and provides oversight for physical security upgrades to over 100 Department facilities throughout the United States.
- b. Develops domestic security policies, procedures and guidelines for protecting Department personnel, facilities, and classified operations in

accordance with standards provided by the Department of Homeland Security (DHS) (Interagency Security Committee).

- c. Conducts security surveys and inspections of all Department domestic facilities to ensure compliance with established Department regulatory guidance and other applicable federal security guidelines.
- d. Coordinates with the Bureau of Administration, Office of Real Property Management (A/OPR), GSA and commercial contractors to ensure that security installations are completed on schedule in compliance with domestic security requirements and design specifications.
- e. Coordinates with A/OPR, GSA and commercial contractors relative to funding security projects relating to installation of security systems and equipment, supporting infrastructure, secure procurement and storage, Construction Surveillance Technicians (CSTs).
- f. Provides security review of A/OPR domestic construction projects, relocations, and renovations of Department office spaces and facilities. Designs security features for upgrades, prioritizes the projects in consultation with A/OPR, and coordinates their funding with requesting Department bureaus.
- g. Evaluates and assesses relevant Department of State and Department of Homeland Security (DHS) threat information relative to domestic facilities.

1 FAM 263.1-2(A) Project Coordination Branch (DS/FDS/PCB)

(TL:ORG-142; 09-28-2005)

- a. Directs, manages, and provides project management oversight for physical security upgrades to Department domestic facilities designated security Levels I - IV by the Department of Justice.
- b. Proposes improvements to physical security systems and equipment to ensure the protection of life, information, and property, while ensuring facility compliance with Department security goals, objectives and regulatory guidance.
- c. Coordinates closely with General Services Administration (GSA) and the Department's of Administration on projects requiring the design and installation of security systems, such as proprietary alarm; automated access control, including vehicle barrier systems; closed circuit television (CCTV); and high security locking hardware.

- d. Provides oversight on the development of Memoranda of Agreements (MOA) for interagency transfer of support funds, and tracking of the reimbursement of funds from other Department entities to ensure the completion of security projects.
- e. Provides construction security for security upgrades in sensitive areas of Department domestic facilities.
- f. Reviews and assesses the results of security surveys and inspections of domestic facilities, including field and passport offices, regional centers, and DOJ designated Level I - IV facilities. Recommends cost-effective countermeasures to eliminate vulnerabilities and hazards. Coordinates funding, prioritization, and drafts the statements of work (SOW) to implement the installation of countermeasures.
- g. Reviews Level I-IV A/OPR new construction and renovation projects of domestic office space and facilities. Assists A/OPR in the prioritization of projects and coordinates their funding with the requesting Department of State bureau.
- h. Designs and integrates intrusion detection systems, access control systems, closed circuit television systems, and high-security locking hardware configurations in conjunction with security upgrades and office renovations.
- i. Coordinates the inclusion of security requirements in the construction drawings and specifications with A/OPR, GSA, and commercial contractors.
- j. Tests and evaluates newly installed physical security equipment to ensure that it meets Department security and operational requirements.

1 FAM 263.1-2(B) Domestic Buildings Branch (DS/FSD/DBB)

(TL:ORG-142; 09-28-2005)

- a. Designs the installation of intrusion detection systems, access control systems, closed circuit television systems, and high-security locking hardware for domestic facilities.
- b. Provides oversight on security requirements for major long-term technical and physical security renovation projects at all DOJ designated Level V Department facilities throughout the United States (Harry S Truman Building, Blair House, and U.S. Mission to the United Nations).

- c. Coordinates the inclusion of security requirements in the construction drawings and specifications with A/OPR, GSA, and commercial contractors.
- d. Provides classified drawings and specifications of facility renovations to construction project managers, coordinators and construction surveillance technicians.
- e. Ensures that commercial contractors comply with Department regulatory requirements during construction.

1 FAM 263.1-2(C) Security Standards and Compliance Branch (DS/FSD/SSC)

(TL:ORG-142; 09-28-2005)

- a. Conducts evaluations, surveys, and inspections of Department domestic facilities to ensure compliance with Department policies, procedures, and guidelines.
- b. Develops and maintains domestic security policies, procedures and guidelines in concert with Interagency Security Committee standards for protecting Department personnel, facilities, and national security information.
- c. Evaluates technical and terrorism threat information and vulnerabilities relative to domestic facilities.
- d. Proposes improvements on the use of physical and technical security systems and certifies their use.
- e. Conducts quarterly alarm testing of the Department's classified processing areas to ensure they meet regulatory guidelines.

1 FAM 263.1-3 Defensive Equipment and Armored Vehicle Division (DS/PSP/DEAV)

(TL:ORG-142; 09-28-2005)

- a. Evaluates, procures, and supplies all defensive and special security equipment required by security personnel at overseas locations.
- b. Manages the armored vehicle program which provides for the:
 - (1) Acquisition and secure movement of all protective vehicles and equipment;

- (2) Armoring of Department (A/LM, MSG, COM) and ICASS security vehicles; and
 - (3) Procurement, product integrity, and deployment abroad of the Department's armored vehicles.
- c. Tests and evaluates defensive equipment.
 - d. Represents the Department on U.S. Government interagency committees involved in developing uniform security standards for defensive equipment and armored vehicles.

1 FAM 263.2 Office of Security Technology (DS/C/ST)

(CT:ORG-149; 02-16-2006)

- a. Provides management and policy direction to the Countermeasures Program Division (DS/ST/CMP), the Security Technology Operations Division (DS/ST/STO), and the Facility Security Engineering Division (DS/ST/FSE).
- b. Directs the development of standards, policies, and procedures associated with technical countermeasures, TEMPEST, security technology operations, and facility security engineering programs domestically and abroad. Ensures that security standards for these disciplines are met to protect national security information, diplomatic facilities, and personnel abroad.
- c. Directs the implementation of technical countermeasures, TEMPEST, security technology operations, and facility security engineering programs.
- d. Develops and implements procedures to track facility profiles, post compliance with Overseas Security Policy Board (OSPB)-approved security technology standards, and exceptions to the OSPB standards.
- e. Directs implementation of DS research and development programs to identify technical countermeasures and DS-approved technical security equipment. Fields approved technical security equipment and maintains an equipment lifecycle.
- f. Represents the Department in intergovernmental and interagency organizations and specialized groups on matters relating to security technology programs.

- g. Coordinates all briefing papers and related materials concerning security technology programs abroad for DS and senior Department management.

1 FAM 263.2-1 Countermeasures Program Division (DS/ST/CMP)

(CT:ORG-149; 02-16-2006)

- a. Provides management and policy direction to the Emanations Countermeasures Branch (DS/CMP/ECB), the Technical Analysis Branch (DS/CMP/TAB), the Technology Evaluation Branch (DS/CMP/TEB), and the Technical Surveillance Countermeasures Branch (DS/CMP/TSC).
- b. Provides Special Access Program (SAP) management.
- c. Serves as the Department's voting member to the Technical Threat Working Group (TTWG).
- d. Serves as the principal liaison to the foreign government members of the International Technical Security (INTECSEC) Group.
- e. Sponsors the INTECSEC security officer exchange program.

1 FAM 263.2-1(A) Emanations Countermeasures Branch (DS/CMP/ECB)

(CT:ORG-149; 02-16-2006)

- a. Represents the Department on the National TEMPEST Advisory Group (TAG) to provide input for the development of national TEMPEST policy for U.S. Government agencies operating domestically and abroad.
- b. Performs TEMPEST countermeasures reviews to determine TEMPEST countermeasures requirements domestically and abroad. Performs TEMPEST inspections worldwide to ensure Department compliance with national emanations standards.
- c. Manages DS's certified shielded enclosure (CSE), built-in conference room (BCR), and secure conference room (SCR) programs. Provides preventive maintenance for DS-owned enclosures and conference rooms and certifies all shielded enclosures and conference rooms worldwide.
- d. Approves Secret-level collateral secure video teleconferencing facilities abroad.

1 FAM 263.2-1(B) Technical Analysis Branch (DS/CMP/TAB)

(CT:ORG-149; 02-16-2006)

- a. Works with the Center for Security Evaluation to evaluate and implement a risk management program designed to identify the specific countermeasures needed to protect classified and sensitive information.
- b. Collects and analyzes information regarding technical threats to Department facilities abroad, security systems, and information systems.
- c. Analyzes technical anomalies at a 24-hours a day, seven days a week security monitoring and analysis center (SMAC) located at the DS Command Center.
- d. Provides input and representation to the Center for Security Evaluation through the Technical Threat Working Group (TTWG) to determine the level of technical threat and degree of risk to national security information at each U.S. diplomatic facility abroad.
- e. Provides guidance, collection, and intelligence analysis of technical security assessments (TSAs), technical surveillance countermeasures (TSCMs), communications security (COMSEC) audits, and technical security reporting.
- f. Manages the COMSEC facility technical inspections program in accordance with the Foreign Affairs Manual (FAM), the Foreign Affairs Handbooks (FAHs), and national policy guidance.

1 FAM 263.2-1(C) Technology Evaluation Branch (DS/CMP/TEB)

(CT:ORG-149; 02-16-2006)

- a. Manages the security risk evaluation and approval process for the introduction of new information and telecommunications technology and equipment into the Department's facilities abroad.
- b. Reports on emerging technology trends and provides analysis pertinent to the Department.

1 FAM 263.2-1(D) Technical Surveillance Countermeasures Branch (DS/CMP/TSC)

(CT:ORG-149; 02-16-2006)

- a. Conducts global TSCM inspections in coordination with DS/ST/STO and DS/ICI/CI.
- b. Serves as the Department's central coordinator for TSCM operations.
- c. Manages TSCM programs and provides resources and services to reduce the risk of technical penetrations or technical hazards in Department of State facilities domestically and abroad.
- d. Ensures that all technical penetrations and technical hazards discovered at U.S. facilities abroad under the umbrella of the chief of mission are reported in coordination with DS/DO/ICI to the Directorate of Central Intelligence (DCI) in accordance with DCI Procedural Guides 1, 2, 3.
- e. Ensures that all technical penetrations discovered at domestic Department of State facilities are reported in coordination with DS/DO/ICI to the Federal Bureau of Investigation.
- f. Provides centralized support for TSCM equipment, including procurement, inventory tracking, development, certification, and repair.

1 FAM 263.2-2 Security Technology Operations Division (DS/ST/STO)

(CT:ORG-149; 02-16-2006)

- a. Provides management and policy direction to the Naval Support Unit (DS/STO/NSU), the Overseas Support Branch (DS/STO/OSB), and the Security Engineering Services Branch (DS/STO/SES).
- b. Directly supervises the OSB and SES branch chiefs and five regional directors for security engineering (RDSEs). RDSEs serve as field managers and the interface between DS and engineering services centers (ESCs) and engineering services offices (ESOs).

1 FAM 263.2-2(A) Naval Support Unit (DS/STO/NSU)

(CT:ORG-149; 02-16-2006)

Supports the Department security engineering program abroad, and

provides Seabee assets for DS and other U.S. Government projects under the terms of a memorandum of understanding (see 12 FAM 451, exhibit 451.5).

1 FAM 263.2-2(B) Overseas Support Branch (DS/STO/OSB)

(CT:ORG-149; 02-16-2006)

- a. Manages, coordinates, and supports the worldwide activities of technical security personnel abroad. These personnel are stationed in U.S. missions, in larger security ESCs, or smaller ESOs.
- b. Prioritizes, obtains, coordinates, and disburses resources to support offices abroad. Resources include positions, travel money, local operating funds, and vehicles.
- c. Develops operational policy and procedures for technical security support.
- d. Coordinates NSU security operations abroad.
- e. Coordinates with regional directors in DS/DSS/IP, executive directors in regional bureaus, post management officers, desk officers in OBO/PE/SM, and others within the Department and in other agencies, on technical security operations and support abroad.
- f. Prepares briefing materials to the Office of the Inspector General (OIG) recommendations on technical security issues of an operational nature. Personnel may also participate in special project coordination and support as directed by DS management.
- g. Serves as the central repository for ESC/ESO reporting, to include technical security surveys and inspections.

1 FAM 263.2-2(C) Security Engineering Services Branch (DS/STO/SES)

(CT:ORG-149; 02-16-2006)

- a. Performs TSCM inspections at domestic facilities.
- b. Conducts sensitive compartmented information facility (SCIF) accreditation surveys in support of the Department's Special Security Office (DS/IS/SSO).
- c. Provides TSCM support for special missions and classified conferences.

- d. Manages the technical security support program for the Secretary of State traveling mission. Develops, procures, and deploys technical security equipment specifically for the Secretary of State support mission. Coordinates among field offices to provide personnel, equipment, and technical security support for the Secretary of State when traveling abroad.
- e. Provides technical security support for the protection of visiting dignitaries and international conferences such as United Nations General Assembly (UNGA), Economic Forum, and Peace Talks.
- f. Provides technical support to DS/DO/ICI in conducting criminal investigations.

1 FAM 263.2-3 Facility Security Engineering Division (DS/ST/FSE)

(CT:ORG-149; 02-16-2006)

- a. Provides management and policy direction to the Domestic Management and Engineering Branch (DS/FSE/DME), the Field Support Branch (DS/FSE/FSB), the Project Management and Engineering Branch (DS/FSE/PME), and the Technology Development Branch (DS/FSE/TDB).
- c. Verifies all DS-funded technical security systems are installed free of defect under existing DS installation standards and regulations.

1 FAM 263.2-3(A) Domestic Management and Engineering Branch (DS/FSE/DME)

(CT:ORG-149; 02-16-2006)

- a. Provides maintenance and repair support for all Department technical security equipment installed domestically.
- b. Manages the design, engineering, and installation of DS-approved facility security equipment as part of new technical security installations and technical security upgrades (TSUs) domestically. This includes coordination of project schedules and priorities, review and approval of technical designs, and development of bills of materials.
- c. Supports DS/STO/SES with technical security support for the Secretary of State residence, Presidential guesthouse, and visiting dignitaries and international conferences.

1 FAM 263.2-3(B) Field Support Branch (DS/FSE/FSB)

(CT:ORG-149; 02-16-2006)

- a. Provides logistical support, including order processing, procurement, warehousing, shipment, and lifecycle management for technical security equipment worldwide.
- b. Manages the Security Equipment Maintenance Program (SEMP) to augment maintenance of security equipment.
- c. Reviews bills of material for the installation of technical security systems at facilities where DS has security responsibility.

1 FAM 263.2-3(C) Project Management and Engineering Branch (DS/FSE/PME)

(CT:ORG-149; 02-16-2006)

- a. Manages the design, engineering, and installation of DS-approved facility security equipment as part of new technical security installations and TSUs abroad. This includes coordination of project schedules and priorities, review and approval of technical designs, development of bills of materials, coordination of funding, and collaboration with other offices.
- b. Reviews bills of material for the installation of technical security systems, developed by the ESC/ESO and approved by the regional security officer (RSO), at facilities where DS has security responsibility.
- c. Verifies all technical security systems are installed free of defect under exiting DS installation standards and regulations.

1 FAM 263.2-3(D) Technology Development Branch (DS/FSE/TDB)

(CT:ORG-149; 02-16-2006)

- a. Identifies, evaluates, develops, and approves technical security equipment.
- b. Writes and publishes the Technical Security Installation Standards Handbook, Application and Installation Guidelines, and Technical Bulletins.
- c. Provides technical assistance and guidance relating to DS-approved

security systems.

- d. Reviews and updates technical security installation standards in the FAH/FAM.

1 FAM 263.3 Office of the Diplomatic Courier Service (DS/C/DC)

(CT:ORG-160; 07-06-2006)

- a. Manages and administers the Diplomatic Courier Service and its three regional courier divisions located in Miami, Frankfurt, and Bangkok, and its hub centers at Manama, Helsinki, Pretoria, Abidjan/Dakar, and Seoul.*
- b. Provides secure and expeditious transmission of classified and sensitive correspondence, equipment, and materials worldwide, in support of the Department of State and the foreign affairs community.*
- c. Formulates, coordinates, and implements policies, plans, and operational procedures for the Diplomatic Courier Service.*
- d. Provides liaison to the courier services of foreign governments, other nations, and international organizations.*
- e. Provides secure control and transport of unclassified but sensitive items or materials designated for use in construction projects abroad and non-consumables for controlled-sensitive areas of U.S. embassies and consulates.*
- f. Oversees Military Support Flights that deliver outsized courier material in support of world wide regional posts.*
- g. Operates the classified pouch vault and performs pouching functions traditionally assigned to the Information Programs Center at some regional and HUB locations where DS/C and IRM concur.*

1 FAM 264 DIRECTOR, OFFICE OF FOREIGN MISSIONS (DS/OFM)

(TL:ORG-89; 08-28-2000)

- a. Exercises authority for the Under Secretary for Management to perform functions vested in the Secretary of State by Title II of the State Department Basic Authorities Act of 1956, as amended and delegated to

M.

- b. Provides for the formulation and implementation of policy designed to provide for reciprocity of treatment between U.S. missions abroad and foreign missions in the United States.
- c. Co-chairs, with the Chief of Protocol (S/CPR), the Accreditation Review Panel, which reviews the status of, activities of and policies applying to foreign diplomats, consular officials, and foreign government offices within the United States to ensure that such activities are in compliance with applicable laws and are not prejudicial to U.S. interests or to the welfare of the local communities in which foreign officials work and live. The Panel assists Federal, state, and local authorities in understanding and granting to foreign diplomatic and consular personnel the privileges and immunities required by international law.
- d. Implements policies, based upon reciprocity and national interests, with regard to the acquisition of benefits, as defined by the Act, by foreign missions in the United States, and deals with representatives of these missions in implementing such policies. These policies include, but are not limited to:
 - (1) Tax Exemptions;
 - (2) Procedures pertaining to foreign mission official and personal travel and accommodations;
 - (3) Real estate acquisition, use disposition, alteration, lease or sale;
 - (4) Licensing and insuring motor vehicles; issuing driver licenses; enforcing compliance with applicable motor vehicle laws and regulations; and working closely with law enforcement agencies in protecting the public from unsafe foreign mission drivers;
 - (5) Assistance in securing staff, services, public utilities, and other benefits;
 - (6) Customs clearances;
 - (7) Deterring, detecting, and penalizing fraud and abuse in the obtaining and use of diplomatic or consular privileges, immunities, and other benefits; and
 - (8) Such other matters as the Secretary may from time to time determine as appropriate.
- e. Provides approval or determinations under the Foreign Missions Act

regarding rights or benefits sought by or made available to foreign missions, including but not limited to the opening, use, maintenance, and operations of foreign missions.

- f. Coordinates with Department offices and functional and regional bureaus on reciprocity and related national security matters, in particular with the Office of Protocol, the Office of the Legal Adviser and the Bureaus of Intelligence and Research and International Organizations, and the U.S. Mission to the United Nations. Coordinates with other interested Federal agencies on similar matters.
- g. Works with state, county, and local officials concerned with issues arising under the Act, including but not limited to the location, size, operations, and conduct of foreign missions.
- h. Coordinates with other public and private agencies that are involved in matters arising under the Act.

1 FAM 264.1 Authorities

(TL: ORG-128; 10-09-2003)

The Foreign Missions Act (Public Law 97-241; 22 U.S.C. 4301, et. seq. (1982)), as amended, authorizes the Secretary of State to designate an office to carry out the purposes of the Act. The Secretary of State's Delegation of Authority No. 147, dated September 13, 1982, delegates functions authorized under the Act to the Under Secretary for Management. Delegation of Authority No. 214, dated September 20, 1994, further delegates functions authorized under the Act, except those under sections 203(4), 204(b)(5), 204(f), 209, 209A, and 214, to the Director of the Office of Foreign Missions.

1 FAM 264.2 Deputy Assistant Secretary, Office of Foreign Missions (DS/OFM)

(TL:ORG-89; 08-28-2000)

- a. Serves as the Deputy Director of the Office of Foreign Missions and oversees the day-to-day operations of DS/OFM's programs.
- b. Formulates policies and implements programs that impact foreign missions in the United States in the areas of tax, property transactions, customs, travel, vehicle ownership and usage, and ensures that these policies and programs work to enhance the treatment of U.S. diplomatic and consular personnel abroad with respect to benefits, privileges and

immunities, and that they conform to overall U.S. foreign policy goals.

- c. Establishes operational procedures to fulfill national security requirements mandated by the Foreign Missions Act and coordinates DS/OFM activities and programs with appropriate national security agencies.
- d. Raises reciprocity and national security issues with State Department bureaus and concerned offices in the intelligence community to assure that these issues are given appropriate consideration in the development and implementation of U.S. foreign policy.
- e. Supervises the DS/OFM Legal Counsel, who provides advice to the Director and Deputy Director, as well as legal support to other elements of DS/OFM in legislative, regulatory, and procedural matters, in coordination with the Office of the Legal Adviser.
- f. Provides direct management oversight to the following DS/OFM offices:
 - (1) Travel, Property and Banking (DS/OFM/TPB);
 - (2) Vehicles, Tax and Customs (DS/OFM/VTC);
 - (3) Regional Offices (DS/OFM/NY, DS/OFM/CH, DS/OFM/LA, and DS/OFM/SF);
 - (4) Information Management (DS/OFM/IM); and
 - (5) Administration (DS/OFM/AO).

1 FAM 264.2-1 Office of Travel, Property and Banking (DS/OFM/TPB)

(TL:ORG-89; 08-28-2000)

- a. Manages acquisitions, alterations, and sales of real property by foreign missions to ensure these are consistent with national security interests, reciprocity and applicable international and domestic law;
- b. Provides guidance to foreign missions and to state and local governments on real property taxation, zoning, and other related matters;
- c. Acts as custodian for foreign mission properties of certain countries with which the United States no longer maintains diplomatic relations or which have recalled their diplomatic missions; and
- d. Manages travel restrictions and controls on foreign missions for reasons of national security or reciprocity.

1 FAM 264.2-2 Office of Vehicles, Tax and Customs (DS/OFM/VTC)

(TL:ORG-89; 08-28-2000)

- a. Manages the Diplomatic Motor Vehicle (DMV) Program and the tax and customs programs.
- b. Directs the development of standards, policies and procedures, and conducts negotiations, to persuade foreign governments to eliminate unwarranted taxation and motor vehicle and customs restrictions imposed on U.S. diplomatic and consular missions and their personnel.

1 FAM 264.2-3 Vehicles Division (DS/OFM/VTC/V)

(TL:ORG-89; 08-28-2000)

- a. Operates the Diplomatic Motor Vehicle (DMV) Program, which does the following:
 - (1) Registers and licenses motor vehicles that belong to foreign missions and their members;
 - (2) Issues driver licenses to members of the foreign mission community and their families;
 - (3) Enforces mandatory insurance standards;
 - (4) Monitors driving records and ensures that foreign mission members who are serious violators do not continue to drive; and
 - (5) Imposes motor vehicle surcharges and limits on foreign missions and their members, based on reciprocity.
- b. Encourages state and local governments to report reckless or negligent incidents by foreign mission drivers; educates them on the protections that immunity gives diplomats and consular officials, and what they legally can do with a foreign mission member who breaks the law.
- c. Tracks and assists with the collection of parking fines incurred by foreign mission members in any U.S. locality which has requested DS/OFM's assistance and cooperation; informs the missions of serious parking abuses; and reports serious fines to the U.S. Congress.

1 FAM 264.2-4 Tax and Customs (DS/OFM/TC)

(CT:ORG-146; 11-23-2005)

- a. Manages reciprocity with the purpose of obtaining advantageous tax and custom policy and practice for U.S. missions and eligible personnel abroad by applying a similar level of tax relief to host governments' missions and their members assigned to a mission in the U.S., in accordance with the Vienna Conventions on Diplomatic and Consular Relations, other bilateral agreements, customary international practice and domestic law.
- b. Ensures the provision of exemption from taxes and duties imposed on the purchases or importations of foreign missions and their members in the United States in accordance with the reciprocal requirements mandated by the U.S. Foreign Missions Act, the Vienna Conventions on Diplomatic and Consular Relations, customary international practice, other bilateral agreements and domestic law.
- c. Assists U.S. missions with obtaining tax/duty relief on purchases of goods and services associated with the operation and management of diplomatic and consular operations and activities abroad, which includes the construction and renovation of diplomatic and consular properties as well as tax and/or duty-free issues associated with the provision of foreign assistance grants. In addition, DS/OFM/TC assists U.S. missions in negotiations with foreign governments with the purpose of establishing agreements that will eliminate or reduce taxes and customs duties imposed on the personal purchases or importations of U.S. mission members abroad.
- d. Facilitates the expeditious import and export of foreign mission materials and the possessions of members of the foreign mission community, based on international and domestic law.
- e. Monitors the policies of foreign governments pertaining to the transport and handling of diplomatic pouches destined for U.S. missions abroad, in accordance with the Vienna Conventions on Diplomatic and Consular Relations, customary international practice and domestic law.

1 FAM 264.3 Regional Offices

(TL:ORG-128; 10-09-2003)

- a. DS/OFM has six regional offices in the United States. They perform the following duties:

- (1) Administer DS/OFM's property, travel, vehicles, tax, and customs programs for foreign missions located within each region to ensure program compliance and national security interests;
- (2) Advise, assist and perform liaison functions with Federal, state, and local government agencies, businesses, and interested individuals within each region, regarding the privileges, benefits, and immunities of foreign missions and of the missions' employees and their dependents, and with respect to alleged violations of law on the part of such persons; and
- (3) Advise foreign missions within each region in matters that will assist them to operate and live in the United States.

b. The DS/OFM regional offices are located in:

- (1) New York (DS/OFM/NY);
- (2) Chicago (DS/OFM/CH);
- (3) Los Angeles (DS/OFM/LA);
- (4) San Francisco (DS/OFM/SF);
- (5) Miami (DS/OFM/MI); and
- (6) Houston (DS/OFM/HU).

1 FAM 264.3-1 Information Management Office (DS/OFM/IM)

(TL:ORG-89; 08-28-2000)

Provides consolidated automated systems support for DS/OFM, including word and data processing, hardware, software, and telecommunications services.

1 FAM 264.3-2 Administrative Office (DS/OFM/AO)

(TL:ORG-89; 08-28-2000)

Provides administrative services to DS/OFM, including:

- (1) Contracting;
- (2) Administration of custodial bank accounts;

- (3) Formulation of DS/OFM budget and financial plan requirements;
and
- (4) General services support.

1 FAM 265 EXECUTIVE DIRECTOR FOR DIPLOMATIC SECURITY (DS/EX)

(CT:ORG-160; 07-06-2006)

- a. Serves as the principal adviser to the Assistant Secretary for Diplomatic Security on management, policy, administrative, planning, and resource issues.
- b. Provides executive direction and management oversight to:
 - (1) Office of Management Services (DS/EX/MGT);
 - (2) Office of the Chief Financial Officer (DS/EX/CFO); and
 - (3) Office of the Chief Technology Officer (DS/EX/CTO).
- c. Develops and implements administrative and management policies, plans, and procedures to ensure that DS resources are allocated, administered, and accounted for in accordance with U.S. Law and Government regulations.
- d. Develops and implements the priorities and program objectives of the Assistant Secretary of DS, using principles of efficient and cost effective management and internal controls.
- e. Provides centralized administrative services, including financial management, contractual and procurement management, personnel management, general services, and automated systems.

1 FAM 265.1 Office of Deputy Executive Director and Management Services (DS/EX/MGT)

(CT:ORG-156; 05-10-2006)

Provides comprehensive management and administrative services to DS, including:

- (1) Administrative, logistics, and general services;

- (2) Contracting and procurement services;
- (3) Policy analysis and planning;
- (4) Human resources management; and
- (5) Serves as Deputy to the Executive Director.

1 FAM 265.1-1 Logistics Services Division (DS/EX/MGT/LS)

(CT:ORG-156; 05-10-2006)

Provides a full range of administrative and logistics services to the Bureau, including:

- (1) Facilities and space planning including design, construction oversight, installation, cost estimates, preparing Charters, maintenance and parking control;
- (2) Property management for domestic and overseas Administrative and Program property;
- (3) Motor vehicle management for the General Services Administration (GSA) and commercial leased vehicles including, accident reporting, tort claim processing, acquisition, disposal, maintenance and Fleet card oversight;
- (4) Administration of the Department's Travel Management program to include travel authorizations, vouchers, training and control;
- (5) Government Travel Card Program management;
- (6) Copier management program; and
- (7) Coordination of other domestic administrative programs.

1 FAM 265.1-2 Contracting and Procurement Division (DS/EX/MGT/CAP)

(CT:ORG-156; 05-10-2006)

Provides a full range of acquisition and procurement services to the Bureau leading to the acquisition of supplies, services and equipment, Interagency Acquisition Agreements (IAAs), Personal Service Contracts (PSCs), credit card purchases, and Federal Assistance Awards;

- (1) Coordinates and processes all DS initiated procurements including requisitions and small purchases (e.g., credit card, contracts, delivery orders and blanket purchase orders);
- (2) Develops (and/or assists in the development of), personal service contracts, statements of work, justifications and approvals (J&A) for sole source requirements, and determinations and findings (D&F) for claims arising from unauthorized commitments/ratifications and proposals;
- (3) Develops, negotiates, awards, administers and interprets policy for all DS Federal Assistant Awards (Grants and Cooperative Agreements);
- (4) Administers and supplements administration of Personal Service Contracts, Interagency Acquisition Agreements (IAA) and resultant Military Interdepartmental Purchase Requests (MIPRs), contracts, etc.;
- (5) Provides technical advice and guidance to Bureau program offices in recommending the best procurement/contracting approach;
- (6) Manages DS active contracts including delivery order preparation requests;
- (7) Provides government purchase card administration and oversight.

1 FAM 265.1-3 Policy and Planning Division (DS/EX/MGT/PPD)

(CT:ORG-156; 05-10-2006)

a. Responsible for:

- (1) Developing, clearing and coordinating policy;
 - (a) Coordinates Bureau changes to the Foreign Affairs Manual (FAM), including drafting, clearance, and final approval of Volume 12 entitled Diplomatic Security (DS), and its accompanying Foreign Affairs Handbooks (FAH);
 - (b) Provides assistance in policy development to DS program offices and senior managers;
 - (c) Facilitates inter- and intra-agency committees, councils, and working groups; and

- (d) Functions as the primary liaison with other agencies and organizations.
- (2) Developing, maintaining and evaluating strategic plans and performance measurement systems;
 - (a) Develops and manages the Bureau's operational and strategic planning, program management, and performance measurement programs to integrate policy initiatives, organizational goals, and post and program requirements with resource availability;
 - (b) Prepares the DS Bureau's annual performance plans and works with the Office of Strategic and Performance Planning to incorporate portions into Department-wide plans and to prepare Performance Accountability Reports for the Office of Management and Budget (OMB) and Congress;
 - (c) Works with OMB to apply the Performance Assessment Rating Tool (PART) to Bureau programs;
 - (d) Coordinates and monitors Bureau compliance with the Federal Managers Financial Integrity Act; and
 - (e) Coordinates vulnerability assessments and internal control reviews; evaluates proposed Bureau corrective actions to ensure they represent an effective and cost beneficial approach for resolving identified weaknesses or vulnerabilities; and tracks and monitors the implementation of all corrective actions.
- (3) Responding to legislative and interagency issues; and
- (4) Developing all memoranda of understanding/agreement on behalf of the Bureau with other Department offices and Federal, state and local government agencies.
- b. Coordinates diplomatic security and countermeasures policy issues with all elements of the Department and other foreign affairs agencies.
- c. Serves as the Executive Secretariat for the Overseas Security Policy Board and Firearms Policy and Review Board and coordinates all activities of the boards, the various working group standards development activities and assists in the resolution of difficult issues between agencies.
 - Develops and issues security standards in coordination with appropriate Department bureaus and the interagency Overseas

Security Policy Board (OSPB).

- d. Oversees the Bureau's compliance with the Office of Inspector General (OIG) and Government Accountability Office (GAO) audits and inspection recommendations, and Accountability Review Board (ARB) recommendations.

1 FAM 265.1-4 Human Resources Management Division (DS/MGT/HRM)

(CT:ORG-156; 05-10-2006)

- a. Advises and makes recommendations to Senior Bureau management, the Executive Director and Deputy Executive Director concerning all aspects of the DS Bureau's human resource management policies and programs; develops programs and implements the DS Bureau's human resource management policies and procedures.
- b. Provides a full range of human resource management services to the Bureau including, for example, recruitment and staffing, classification, compensation, training and development, employee relations, performance management, employee benefits and services.
- c. Provides workforce analysis, organizational planning and position management services, worldwide, to DS Bureau management on the domestic DS Bureau workforce, and the overseas workforce identified as Special Agents, Security Engineering Officers, Security Technical Specialists and Diplomatic Couriers.
- d. Administers programs for the recruitment and examination of candidates for security-related Foreign Service positions, Personal Service Contractors, and Law Enforcement Availability Pay.
- e. Makes decisions concerning Civil Service staffing and classification and recommends action to the Executive Director regarding employee relations cases from entry level through the GS-13 level, through Delegation of Personnel Authority from the Director General of the Foreign Service and the Director of Human Resources.
- f. Analyzes and evaluates the effectiveness of the DS Bureau's Human Resource Management Program.
- g. Acts as consultant to both management and employees about any issue concerning human resource management, policies, programs, or procedures.

1 FAM 265.2 Office of the Chief Financial Officer (DS/EX/CFO)

(CT:ORG-156; 05-10-2006)

- a. Directs all aspects of the Bureau of Diplomatic Security's (DS) financial resources.
- b. Acts as the primary liaison between DS and the Bureau of Resource Management (RM/CFO, RM/F/DFCO, RM/BP, and RM/FA).
- c. Participates in the program planning process to facilitate estimation of future resource needs commensurate with policy goals and objectives.
- d. Develops and implements strategies for the most effective and persuasive presentation of budget requests for increased funding as part of the Department's budget submission to OMB, and the President's Budget to Congress.
- e. Coordinates with and advises DS program managers and senior officials on all budget and financial matters.
- f. Prepares the annual financial plan for all DS operating accounts.
- g. Requests and justifies additional resources for any unforeseen emergent unfunded requirements within the D&CP appropriation, as part of the Department's annual financial planning and quarterly review process or emergency supplemental request to Congress.
- h. Monitors the execution of approved financial plans and recommends the reprogramming of resource allocations to the bureau's Resource Board throughout the fiscal year.
- i. Oversees the transfer of appropriated funds and reimbursements and helps to develop and negotiate agreements with other bureaus and other U.S. Government agencies pertaining to both.
- j. Certifies funding availability for all obligations (i.e., travel authorizations, procurement actions, etc.) and provides fiscal data for obligating documents.
- k. Maintains appropriate management and internal control systems to ensure that all financial resources are safeguarded against waste, fraud, unauthorized use, or misappropriation; obligations incurred comply with applicable laws and regulations; and revenues and expenditures are promptly recorded and accounted for in accordance with Departmental

procedures.

- I. Proactively identifies program areas where potential for waste, fraud, unauthorized use or misappropriation of financial resources exists and pursues systematic resolution.

1 FAM 265.2-1 Financial Execution Division (DS/CFO/FE)

(CT:ORG-156; 05-10-2006)

- a. Ensures that obligations incurred comply with applicable laws and regulations; and revenues and expenditures are promptly recorded and accounted for in accordance with Departmental procedures.
- b. Executes the Bureau of Diplomatic Security budget approved by the Congress by:
 - (1) Allotting funds to Foreign Service posts abroad;
 - (2) Certifying funds available for all domestic obligations; and
 - (3) Monitoring the status of worldwide allotments, obligations, and expenditures.
- c. Creates and maintains auditable files for all valid obligations.
- d. Serves as the primary liaison between DS and the Domestic Financial Services Directorate (RM/F/DFS), the Global Financial Management Systems Directorate (RM/F/FMS), the Financial Policy, Reporting and Analysis Directorate (RM/F/FPRA) and the Charleston Financial Services Center (RM/F/CFSC) concerning budget execution matters.
- e. Provides support on all matters relating to the bureau's financial management system. Reviews financial management system changes and enhancements to ensure proper management and accounting controls are maintained.
- f. Performs reconciliation of financial data between the Department's Central Financial Management System (CFMS) and the bureau's financial management system.
- g. Audits domestic financial activity for compliance with bureau policy and applicable laws and regulations.
- h. Identifies, verifies and reports Anti-Deficiency Act violations and institutes corrective action when feasible.

- i. Ensures accuracy, quality, and timeliness of the financial data by tracking and preparing financial management information reports on the status of funds by:
 - (1) Appropriation;
 - (2) Allotment;
 - (3) Obligation;
 - (4) Performance goal; and
 - (5) Sub-objective.
- j. Oversees the interface of the bureau's accounting system and other departmental systems.
- k. Maintains the domestic representational account for the Assistant Secretary reimbursing senior management as per Departmental guidelines for approved representational expenses. Reconciles the representational checking account to bank statements. Keeps accountable records for all disbursements.
- l. Monitors and verifies fiscal information for all purchase card accounts.
- m. Ensures appropriate separation of duties as per regulations and accounting standard operating practices. Reviews and revises internal control processes and streamline financial management processes.
- n. Oversees the transfer of appropriated funds and reimbursements and helps to develop and negotiate agreements with other bureaus and other U.S. government agencies pertaining to both.
- o. Provides data documentation and other support regarding reimbursable earnings to accommodate accounts receivable to ensure collection of earned income.

1 FAM 265.2-2 Financial Planning Division (DS/CFO/FP)

(CT:ORG-156; 05-10-2006)

- a. Safeguards all funds from misappropriation, waste, loss, and unauthorized use in compliance with all applicable laws and regulations.
- b. Plans, develops, presents, justifies, and defends all bureau funding requests to the Department, OMB and Congress.

- c. Coordinates closely with the Bureau of Diplomatic Security's Policy and Planning Office to fully integrate the bureau's planning, budgeting, and performance evaluation process.
- d. Serves as the primary liaison between DS and the Office of State Programs, Operations and Budget (RM/BP), Office of Foreign Assistance Programs (RM/FA), and International Cooperative Administrative Support Services (ICASS) Service Center (RM/BP/ICASS) about budget formulation matters.
- e. Develops long range and integrated financial planning strategies across appropriations that reflect interagency and Departmental coordination within the context of the bureau's overall planning and budgeting functions.
- f. Provides financial estimates as part of the Bureau Program Plan (BPP) process by program performance goals and objectives, object class, program and organization.
- g. Prepares documents for inclusion into briefing packages (i.e., Q&A's on budget issues, funding matrixes, history of funding requests and approvals, etc.) for the participation of DS senior officials in the critical events (i.e., annual Bureau Performance Plan senior review, Congressional testimony, etc.).
- h. Analyzes and evaluates the impact of authorization and appropriation legislation on bureau resources and their allocations.
- i. Organizes and develops the annual financial plan. Analyzes financial plan requests submitted by bureau offices and defends requests submitted to the Department for additional funding.
- j. Monitors the execution of approved financial plan and recommends the reprogramming of resources to the bureau's Resource Board. Submits and defends unfunded requirements to RM/BP during the quarterly review process.
- k. Conducts monthly Resource Board meetings compiling unfunded requests throughout the bureau, creating briefing folders for senior managers with agenda and relevant materials for the meeting.
- l. Allocates DS resources consistent with Departmental and DS policies and objectives, and applicable laws and regulations.
- m. Ensures efficient and effective use of DS resources and analyzes and evaluates their use in accomplishing DS program objectives.

- n. Analyzes funding requirements and expenditure trends in relation to bureau and office functions.
- o. Seeks ways to improve the overall financial management of DS resources to ensure optimal resource management and use through special studies on resource issues addressing strategic planning, resource utilization, and operating requirements.
- p. Coordinates the Bureau's ICASS initial and mid-year budget submissions for the DS Local Guard Program worldwide, identifying and justifying additional funding requirements for each.
- q. Participates in and defends the Bureau's ICASS budget for the Local Guard Program in ICASS Working Group meetings and hearings.
- r. Performs management analyses of ICASS cost data on a macro and post level to derive more efficient and cost-effective management and delivery of local guard services.
- s. Reviews foreign exchange rate allotment adjustments for accuracy and analyzes and estimates the impact of foreign currency fluctuations on DS operations overseas.

1 FAM 265.3 Office of the Chief Technology Officer (DS/EX/CTO)

(CT:ORG-156; 05-10-2006)

- a. Manages the Bureau's program for processing requests for DS documents under the Freedom of Information and Privacy Act (FOIA), and the Bureau's records management program.
- b. Provides consolidated automated systems support for DS, including:
 - (1) Data center operation, help desk, configuration management, and information security;
 - (2) Software development, maintenance, installation, integration, training and support;
 - (3) Data communication, system networking, and video teleconferencing services or solutions; and
 - (4) Capital planning, systems integration, project management, enterprise architecture and system planning, and business analysis and requirements.

1 FAM 265.3-1 Capital Planning and Architecture Division (DS/CTO/CPA)

(CT:ORG-156; 05-10-2006)

- a. Strategically plans and aligns information technology investments to Federal requirements, the Department of State mission, and the goals of DS. This division ensures DS priority investments are planned, funded and managed adequately to accomplish their intended purpose. It is comprised of five functional areas identified below;
- (1) Capital Planning – provides results-oriented information on all matters related to the planning, budgeting, management, and control of IT capital investments including the ongoing evaluation of the existing investment portfolio, and ensuring Bureau compliance with e-Governance reporting guidelines;
 - (2) Systems Integration – designs, evaluates, integrates and implements IT systems solutions for DS;
 - (3) Project Management - responsible for evaluating, planning, organizing and directing all IT projects for the Bureau and ensuring that e-Governance principles are applied to all IT investments;
 - (4) Enterprise Architecture and Systems Planning – develops, maintains and facilitates the implementation of an integrated IT Architecture that aligns technology with business needs, Department of State enterprise architecture and Federal enterprise architecture standards; and
 - (5) Business Analysis and Requirements – reviews current business processes that impact IT projects and elicits, documents and validates requirements of Bureau IT project stakeholders.

1 FAM 265.3-2 Systems Management Division (DS/CTO/SMD)

(CT:ORG-160; 07-06-2006)

Manages DS software development and maintenance, information security, and overall IT operations for the Bureau, including the DS Data Center, network management, and help desk, and designs, develops, and deploys current, advanced technology to meet the Bureau's needs. It contains three functional areas that are described below.

- (1) Operations – operates the 24x7 DS Data Center and data centers in*

other annexes, runs the CTO Help Desk, manages networks, and installs and maintains IT equipment;

- (2) Security Operations – ensures the confidentiality, integrity and availability of DS automated information systems (AIS) by assuring that all systems comply with 5 FAM and 12 FAM regulations and departmental security configuration guidelines, and approves and audits all user accounts; and*
- (3) Software – performs full life cycle management of software design, development, implementation, and maintenance, including database administration and Web and client/server application management, and performs limited end user application training.*

1 FAM 265.3-3 Records Management Division (DS/CTO/RMD)

(CT:ORG-160; 07-06-2006)

- a. Responds to all inquiries assigned to the Bureau under the Freedom of Information Act (FOIA) (5 U.S.C. 552); the Privacy Act (5 U.S.C. 552a); and applicable Executive Orders (EO) for records or information originated by the Bureau. Responds on behalf of the Bureau to special requests for document production and justifies release or denial decisions in the amendment, appeal, and/or litigation processes.*
- b. Provides policy guidelines to Bureau components on information management as mandated by the Privacy Act, the Freedom of Information Act, and applicable executive orders.*
- c. Serves as the Bureau's primary point of contact for customers in matters pertaining to security records life-cycle management, public and need-to-know access to security information, classification management and declassification, privacy, and research of official security records.*

1 FAM 266 SENIOR COORDINATOR FOR SECURITY INFRASTRUCTURE (DS/SI)

(CT:ORG-149; 02-16-2006)

- a. Manages matters relating to security infrastructure in the DS functional areas of information security, computer security, and personnel security and suitability.*

- b. Formulates, consolidates, and recommends to the Assistant Secretary strategic operational planning, priorities, and funding for DS security infrastructure operations.
- c. Chairs and/or serves on Departmental and/or interagency groups and committees relating to security infrastructure.

1 FAM 266.1 Office of Information Security (DS/SI/IS)

(CT:ORG-149; 02-16-2006)

- a. Responsible for the Department's information protection programs, as described in this section and in sections for the Program Applications Division, Industrial Security Division, and the Special Security Operations Divisions (see 1 FAM 266.1-1, 266.1-2, 266.1-3).
- b. Develops, implements, and oversees special access program (SAP) security requirements, to include physical, technical, personnel, Automated Information System (AIS), telecommunications, operational, and procedural.
- c. Coordinates SecState approval of Department-created SAPs and oversees their annual recertification.
- d. Establishes and oversees Foreign Exchange Officer security requirements and security monitoring of the Foreign Exchange Officer local area networks (LANs). Ensures the foreign exchange officers meet all security requirements, and works with IRM/IA to ensure certification and accreditation (C&A) on these LANs.
- e. Conducts comprehensive security vulnerability assessments abroad to determine posts' information and operations security (OPSEC) postures. Assists Regional and Post Security Officers, among others, in establishing effective incident prevention, education and awareness, and strong operations security programs.
- f. Coordinates certification and accreditation actions for all Sensitive Compartmented Information (SCI) systems within a Department facility, domestically, or diplomatic facility, abroad.
- g. Coordinates certification and accreditation actions for Sensitive Compartmented Information Facilities (SCIFs) located in diplomatic facilities abroad.
- h. Develops, implements, and oversees SCI systems policy and procedures.

Serves as the Senior Official of the Intelligence Community (SOIC)'s Designated Accrediting Authority (DAA) for SCI systems and serves as the SOIC representative to security-related Intelligence Community boards and working groups.

- i. Implements and maintains a monitoring center for Department-owned SCI networks' intrusion detection system (IDS). Reports SCI system intrusions and incidents to the SCI system owner and oversees remediation.
- j. Coordinates damage assessments when Department information has been subjected to compromise. Provides investigative and/or prosecutorial support in cases involving unauthorized disclosure or espionage involving Department information or employees. Serves as the Department's security representative on interagency damage assessments team.
- k. Serves as the DS Critical Infrastructure Protection (CIP) coordinator. Represents DS in Department, and other agency forums. Facilitates interagency CIP security discussion and sharing of best practices. Serves as the primary DS interface with the Bureau of Resource Management, the Department's CIP program office.

1 FAM 266.1-1 Program Applications Division (DS/IS/APD)

(CT:ORG-149; 02-16-2006)

- a. Administers the Department's information protection program, as described in this section.
- b. Develops, implements, and oversees policies and procedures for the safeguarding of national security information in accordance with national laws, orders, and directives.
- c. Develops, implements, and oversees policies and procedures for the safeguarding of administratively controlled information designated as Sensitive But Unclassified (SBU).
- d. Provides procedural and operations security direction, guidance, and assistance to all bureaus and posts utilizing e-mail help desks, on-site reviews, security notices, and other available means.
- e. Manages an information and operations security education, training, and awareness program.

- f. Administers the Department's security incident program. Coordinates cases subject to disciplinary action with the Bureau of Human Resources, Employee Relations Division (HR/ER), personnel security clearance actions with DS, and SCI access actions with INR and DS. Conducts incident investigations, to include those involving COMSEC and SCI, and coordinates investigations with DS and other agency investigative elements as required.
- g. Manages the Department's domestic Bureau Security Officer and Unit Security Officer program designed to implement effective internal security controls within the bureaus and throughout the Department.
- h. Develops, implements, and oversees a Department OPSEC program in accordance with national directives. Conducts OPSEC surveys. Provides OPSEC program training.
- i. Develops, implements, and oversees the Department's Top Secret Control Program.
- j. Develops, implements, and oversees the requirements for classified information/operations open storage. Approves all open storage areas/facilities and administers a recertification program.

1 FAM 266.1-2 Industrial Security Division (DS/IS/IND)

(CT:ORG-149; 02-16-2006)

- a. Administers the Department's Industrial Security Program to ensure classified information entrusted to or generated by private industry is properly protected.
- b. Develops and recommends policies, standards, and procedures for the protection of classified information and specifically designated unclassified information provided to Department contractors and consultants.
- c. Analyzes procurement documentation and ensures that appropriate security requirements are incorporated into all contracts in support of the Department's classified and SBU acquisitions.
- d. Develops policies and ensures the implementation of procedures for the disclosure of national security and other sensitive information to firms with significant foreign ownership, control, or influence.
- e. Develops, implements, and administers an industrial security compliance program and conducts inspections of Department contractors to ensure their adherence to Department and national industrial security

requirements.

- f. Serves as the Department's liaison with National Industrial Security Program (NISP) managers and serves as the Department's primary liaison with the Department of Defense and other Federal agencies in administering an effective industrial security program.
- g. Approves cleared visit authorizations for contractor personnel.
- h. Conducts industrial security program briefings for Contracting Officers, Contracting Officers' Representatives, and Program Managers. Provides industrial security briefings and other educational materials to contractor facilities and employees.
- i. Coordinates the security review and analysis of proposed foreign acquisitions of U.S. firms and provides the cleared DS position to the Bureau of Economics and Business Affairs.
- j. Coordinates system connectivity requirements of contractors connecting to Department information systems and oversees compliance. Requirements are established in conjunction with 1 FAM 271.2e(6)(a).

1 FAM 266.1-3 Special Security Operations Division (DS/IS/SSO)

(CT:ORG-149; 02-16-2006)

- a. Develops and implements policies and procedures to ensure that intelligence information, including Sensitive Compartmented Information (SCI), is disseminated and used securely in accordance with Director of Central Intelligence Directives (DCIDs).
- b. Establishes and maintains a secure document control system for SCI materials. Provides for the accountability and control of designated documents. Conducts a continuous review of document flow into, within, and out of the Department. Ensures the timely and secure dissemination of intelligence to Department decision makers.
- c. Develops implementing policies and procedures to protect SCI and SCI-indoctrinated personnel from intelligence or counterintelligence threats as a consequence of hazardous travel in accordance with DCIDs.
- d. Develops, implements, and oversees policies, plans, and procedures for the certification and accreditation of Sensitive Compartmented Information Facilities (SCIFs) in accordance with DCIDs. Serves as the Cognizant Security Authority (CSA) for SCIF accreditation and operations

and coordinates SCIF certification with DCI officials.

- e. Ensures that technical surveillance countermeasures (TSCM) are conducted in all SCIFs in accordance with DCIDs.
- f. Provides SCI security education and awareness for Department personnel. Conducts SCI access indoctrinations and debriefings.
- g. Manages SCI security policies and access control procedures for all SCI facilities. Conducts SCIF Periodic Security Reviews (PSRs).
- h. Reviews and approves physical security pre-construction plans for SCIF construction, expansion, or modification.
- i. Monitors all SCIF construction, expansion, or modification to ensure the integrity of the facility is properly maintained.
- j. Evaluates the outside threat to Department SCIFs and develops policy and standards to better protect SCI material.
- k. Coordinates all requests for SCI access with the SOIC Determination Authority (DA) and DS's Office of Personnel Security and Suitability (DS/SI/PSS). Maintains a database of all Department personnel with SCI access. Inputs records of SCI access into the Intelligence Community global database. Serves as the office of primary responsibility for the passing of SCI accesses through proper channels.
- l. Keeps the Department Senior Official of the Intelligence Community (SOIC), the Assistant Secretary for INR, continually informed and seeks clearance/approval for requisite actions in accordance with DCIDs and the DS-INR Memorandum of Agreement that designates Diplomatic Security as the Cognizant Security Authority (CSA) for intelligence sources and methods security.

1 FAM 266.2 Office of Computer Security (DS/SI/CS)

(CT:ORG-149; 02-16-2006)

- a. Recommends, develops, and coordinates cyber security policy, standards, and guidelines.
- b. Recommends, develops, and coordinates all waivers and exceptions to Department cyber security policy.
- c. Assesses emerging cyber security technology and provides findings to

senior management, including the Chief Information Officer (CIO), the Assistant Secretary for Diplomatic Security, and system owners.

- d. Provides technical expertise to support the Department's information security (INFOSEC) program as it relates to the protection of collateral information.
- e. Conducts site evaluation and verification activities at domestic and abroad locations.
- f. Conducts detailed security and safeguards analyses of software and firmware used in the Department's information technology (IT) systems.
- g. Supports the Senior Coordinator for Security Infrastructure (DS/SI) by updating and documenting computer security program development and changes.
- h. Identifies and implements cyber security technology to support the Department's technical counterterrorism and counterintelligence capabilities.
- i. Manages the Overseas Security Policy Board (OSPB) Information Systems Standards Working Group (ISSWG) for the development of uniform computer security standards for all Foreign Affairs agencies serving under the authority of chiefs of mission.
- j. Approves waivers and exceptions to OSPB standards. Coordinates, in conjunction with IRM, waivers and exceptions to OSPB standards for Department of State elements.
- k. Represents the Department as the primary representative for the Committee on National Security Systems (CNSS), the Intelligence Community, the Department of Homeland Security (on cyber security issues), and the United States Computer Emergency Readiness Team (for cyber incident reporting).
- l. Creates and delivers the cyber security awareness program for all Department users, including system administrators, information systems security officers (ISSOs), and managers and chief executives, briefing them on IT security responsibilities, risks to information and systems, and related policies and controls to mitigate those risks, as approved by the CISO.
- m. Approves the unattended operation of IT systems that process classified information at **CRITICAL THREAT** posts.
- n. Directs, manages, and maintains the Department's overall capacity for

network intrusion detection, monitoring, incident handling and response, and cyber threat analysis. Provides technical analysis and assistance to DS and other Federal law enforcement agencies.

- o. Manages a cadre of U.S. Government IT security specialists to act as regional computer security officers (RCSOs) to provide on-site customer support, training, and oversight to Department employees worldwide.
- p. Provides analysis and assistance to develop unique security solutions to meet the Department's operating requirements and to meet requirements resulting from bureaus' specific requests.
- q. Develops and maintains security configuration standards and guidelines for Departmental implementation of IT hardware and applications. Provides ongoing assistance to Department system managers, applications developers, and Department- and bureau-level configuration control boards to ensure IT security requirements are included in life-cycle management of systems and applications.
- r. Develops and maintains a cyber-threat analysis and reporting capability to support Department-level threat determinations and subsequent vulnerability mitigation.
- s. Coordinates cyber security intelligence sharing and (threat) analysis with the Intelligence Community and Department of Homeland Security.
- t. Conducts continuous and directed network- or application-specific vulnerability assessment testing, independent penetration testing, and intelligence monitoring to identify specific risks to those systems and develop risk mitigation strategies to protect the Department's IT infrastructure.
- u. Develops, in conjunction with IRM/OPS, cyber security procedures for operational elements.
- v. Conducts security analyses, independent vulnerability assessments, and selective cyber security control reviews of IT systems.
- w. Provides oversight for the overall monitoring of Department telecommunications resources, systems, and networks, to include detection and response to security-related incidents involving telephone or telephone equipment.
- x. Provides for the development and use of automated validation tools to perform compliance monitoring and reporting.

1 FAM 266.2-1 Monitoring & Incident Response Division (DS/CS/MIR)

(CT:ORG-149; 02-16-2006)

- a. Maintains a layered intrusion detection system (IDS) program to: monitor and audit network and host information systems; detect inappropriate, incorrect, or anomalous activity; and issue warnings and alerts for possible unauthorized access to the Department's networks and worldwide systems.
- b. Maintains a Computer Incident Response Team (CIRT) to serve as the Department's focal point for reporting computer security incidents impacting Department and Foreign Affairs agency networks. Information about incidents is shared and coordinated with operational managers, law enforcement within DS, and outside agencies as appropriate to support criminal prosecution.
- c. Reports incident information to US-CERT and participates in the quarterly US-CERT Partners meetings where Federal incident response teams, law enforcement, private sector representatives, and academics exchange ideas and examine technical issues. Acts as liaison with other Federal and DoD CERTs for the exchange of information and reporting of computer security incidents.
- d. Determines computer misuse and provides technical assistance for criminal investigations.
- e. Provides and maintains the capability for the overall monitoring of Department telecommunications resources, systems, and networks to include detection and response to security-related incidents involving telephone or telephone equipment. Refers telephone security incidents to the DS investigative authority.

1 FAM 266.2-2 Cyber Threat Analysis Division (DS/CS/CTA)

(CT:ORG-149; 02-16-2006)

- a. Maintains a Cyber Threat Analysis Cell (CTAC) to provide posts abroad and senior Department management with indications and warnings via extensive analysis and reporting of cyber threats impacting the Department's critical infrastructure.
- b. Consolidates and analyzes information and data from the firewall team, Network Monitoring Center, the CIRT, the Intelligence Community, and

other U.S. Government agencies to produce a comprehensive, all-source threat picture of the Department's critical infrastructure.

- c. Serves as the Department's "information broker" for cyber threat information by routinely disseminating cyber threat information to upper management, regional security officers (RSOs), RCSOs, information security officers (ISOs), the Virus Incident Response Team, the CIRT, the Network Monitoring Center, DS/ICI/CI, DS/ICI/CR, and the firewall team.
- d. Helps satisfy Federal information-sharing requirements through active liaison relationships with law enforcement and Intelligence Community entities that have significant cyber security responsibilities, including relationships with the FBI, Department of Homeland Security, Air Force Office of Special Investigations, the Defense Intelligence Agency, CIA, and the DoD Joint Task Force-Global Network Operations (JTF-GNO).
- e. Produces comprehensive cyber threat assessments and analysis regarding State and non-State entities that may pose a threat to the Department's IT infrastructure for the Department's systems and management staff.
- f. Assists in determining the threat posed to the Department's critical IT infrastructure and functions as the Department's all-source fusion cell by merging cyber threat information and analysis.
- g. Produces cyber threat advisories, special reports, and comprehensive threat assessments concerning threats to and potential vulnerabilities of Department networks.
- h. Conducts independent assessments related to vulnerabilities associated with the Department's IT systems.
- i. Identifies vulnerabilities through a combination of assessments and testing of the Department's network resources, including full scope red teaming, penetration testing, and advanced analyses addressing system assets; potential undesirable cyber events; the motives, intentions, capabilities, and history of adversaries; exploiting security weaknesses; risks; and the costs and impacts of countermeasures to ensure integrity of the Department's architecture.
- j. Conducts advanced analyses and trends analysis of malicious activity against the Department's critical infrastructure.

1 FAM 266.2-3 Enterprise Technology, Policy & Awareness Division (DS/CS/ETPA)

(CT:ORG-149; 02-16-2006)

- a. Provides technical expertise in support of the Department's information security program, including developing the technical rationale for changes in INFOSEC policy. Provides specialized technical training to DS personnel, as needed.
- b. Conducts product testing to ascertain security requirements prior to implementation with Department systems or applications.
- c. Provides routine and special network and application vulnerability testing and monitoring.
- d. Arranges and conducts independent penetration testing, with IRM/IA collaboration.
- e. Develops and maintains security configuration standards and guidelines for Departmental implementation of IT hardware and applications.
- f. Provides analysis and assistance to develop unique security solutions to meet Department operating requirements and to meet requirements resulting from bureaus' specific requests.
- g. Develops cyber security procedures for operational elements in conjunction with IRM.
- h. Through the Computer Security Awareness Program, provides timely and accurate guidance to all users ensuring all personnel are aware of current policies and procedures as well as their role and accountability in reducing information security risks associated with their activities. Initiates, develops, disseminates, and provides computer security awareness training to all Department IT users, managers, and operators. CISO approves awareness programs.
- i. Coordinates and develops web-based awareness training targeting users on unclassified and classified systems; newsletters on current information systems security concepts and programs; dissemination of current and new standards and policies; and development of Department notices and worldwide messages on issues of immediate concern to the Department community. CISO approves training curricula.
- j. Recommends, develops, and coordinates clearance of computer, communications, and network security policies, standards, and guidelines.

This policy-related activity covers Computer/Network Security (COMPUSEC) Policy and Standards that define the Department's minimum security requirements for automated information systems (AISs) and AIS networks (local area networks (LANs) and worldwide area networks (WANs) as well as Communications Security (COMSEC) Policy that stipulates security requirements for the environment and the equipment.

- k. Recommends, develops, and coordinates clearance of waivers and exceptions to Department computer, communications, and network security policies.
- l. Chairs the Overseas Security Policy Board's (OSPB) Information Systems Security Working Group (ISSWG), responsible for updating existing 12 FAH-6 H-540 AISs security policies. The group is comprised of members from all U.S. Government agencies that operate in the environment abroad under chief of mission authority.
- m. Assesses emerging cyber security technology and provides findings to senior management, including the Chief Information Officer (CIO), the Assistant Secretary for Diplomatic Security, and system owners.
- n. Conducts detailed security and safeguards analyses of software and firmware used in the Department's IT systems and updates policy, standards, and guidelines as necessary.
- o. Manages, recommends, develops, and coordinates all OSPB waivers and exceptions to classified and unclassified computer security standards.
- p. Recommends and coordinates the approval of domestic, unattended operations of IT systems that process classified information.
- q. Recommends and coordinates the approval of unattended operations of IT systems that process classified information at **CRITICAL THREAT** posts.
- r. Serves as the Department of State Coordinator for the Committee on National Security Systems (CNSS). Reviews, coordinates, and develops the Department's position on national-level classified computer and communications security policies voted upon by the Department's CNSS representative.

1 FAM 266.2-4 Evaluation and Verification Program

(CT:ORG-149; 02-16-2006)

- a. Conducts site evaluation and verification activities at domestic and abroad locations. Advises IRM of site evaluations and verification activities and

obtains CISO clearance/approval as necessary, in accordance with 1 FAM 270.

- b. Conducts site evaluations and verifications of hardware and software used in the Department's computer and communications sites that process classified, unclassified, and Sensitive But Unclassified (SBU) information.
- c. Performs computer, cyber, and communications security evaluations as a function of network and technical assurance.
- d. Conducts site evaluations and verifications to ensure sites are in accordance with national standards and the Designated Approving Authority's authorization decisions. [There are no national standards for E&V]
- e. Provides for the development and use of automated validation tools to perform compliance monitoring and reporting.
- f. Provides management, direction, oversight, leadership, and coordination for the Department's global RCSO. The program manager is responsible for sharing RCSO reporting with the CISO. The RCSO is a Foreign Service security engineering officer (SEO) who has completed the technical security countermeasures training at the Interagency Training Center as well as a formal RCSO training and certification program approved by DS/SI/CS and the DS Training Center (DS/TPS/SECD). Recommended selection of Foreign Service security engineers for assignment abroad as RCSOs is performed by the Program Manager, Evaluations and Verification Program, in coordination with the Office Director for Security Technology (DS/C/ST). The RCSO's duties include the following:
 - (1) Provides quality and timely information systems security support, expertise, and "hands-on" assistance to U.S. missions worldwide to ensure the confidentiality, integrity, and availability of classified and unclassified information systems;
 - (2) Reports to the Program Manager of the Evaluation and Verification Program, on all matters relating to AISs security. The individual implements criteria for access controls, storage, transmission, and destruction of data maintained by AISs at posts and monitors post compliance with those criteria;
 - (3) Conducts on-site AISs security evaluations and verifications of classified and unclassified nonmainframe AISs and prepares formal reports detailing with findings and recommendations;
 - (4) Supplements standard AISs security training materials with specific

information tailored to post's requirements and processing environments and supports contingency planning efforts;

- (5) Performs formal IT security assessments and evaluations on classified and unclassified systems for adherence to regulations, unauthorized connections, and illegal activity. Performs inspections of IT networks to detect whether any of the computer systems or networks at a mission have been compromised;
 - (6) Provides on-site security training and assistance to the ISSOs at each post location. Develops and provides tailored training to the ISSOs to assist them with efficiently accomplishing their tasks in minimal time;
 - (7) Supports the RSOs in investigations involving information systems, including collection of computer forensic images when necessary;
 - (8) Briefs post personnel on IT security initiatives, activities, vulnerabilities, or issues that are specific to the threat level for that post; and
 - (9) As the DS "first responder" to IT security issues at assigned posts, promulgates and disseminates solutions for applications, at the posts within their assigned region, to ensure these applications meet the latest IT security standards.
- g. Establishes working relationships among the Bureau of Information Resource Management (IRM), DS, and post managers to assure security compliance can be obtained while maintaining productivity. Provides advice, consultation, guidance, and information to senior post management officials/staff on the overall computer security posture of post IT systems, implementation of IT security solutions to improve work processes, and resolution of ongoing computer security issues. Provides advice and guidance to post personnel on IT security policy questions from posts within their assigned region.
 - h. Interacts with DS and IRM staff and actively participates in the development of Departmental IT security standards and policies, the exploration of new IT security technologies, and the resolution of IT security enterprise problems.
 - i. Manages, conducts, and coordinates the performance of the Department's site evaluation and verification program and inspections.

1 FAM 266.3 Office of Personnel Security and Suitability (DS/SI/PSS)

(CT:ORG-149; 02-16-2006)

- a. Responsible for the Department's Personnel Security and Suitability programs.
- b. Administers the contract background security investigator program, comprised of over 600 investigators worldwide.
- c. Develops, implements and oversees the Department's policy on personnel security investigations and their subsequent adjudication.

1 FAM 266.3-1 Investigations and Adjudications Division 1(DS/PSS/IA1)

(CT:ORG-149; 02-16-2006)

- a. Conducts personnel security and/or suitability investigations of employees, applicants, contractors, and others seeking access to Department information and/or facilities.
- b. Directs the conduct of such investigations abroad for other Federal agencies.
- c. Conducts file reviews on behalf of the SOIC, in accordance w/DCID 6/4, and recommends eligibility for SCI access to the SOIC DA.
- d. Makes security clearances eligibility determinations and public trust certifications for current employees, applicants for employment, certain contractor personnel in support of the critical mission, and others seeking access to Department information and facilities.

1 FAM 266.3-2 Investigations and Adjudications Division 2(DS/PSS/IA2)

(CT:ORG-149; 02-16-2006)

- a. Conducts personnel security and/or suitability investigations of employees, applicants, contractors, and others seeking access to Department information and/or facilities.
- b. Directs the conduct of such investigations abroad for other Federal agencies.
- c. Conducts reviews on behalf of the SOIC and recommends eligibility for

SCI access to the DA, in accordance w/DCID 6/4 and recommends eligibility for SCI access to the SOIC DA.

- d. Makes security clearance eligibility determinations and public trust certifications for current employees, applicants for employment, certain contractor personnel in support of the critical mission, and others seeking access to Department information and facilities.

1 FAM 266.3-3 Adverse Actions (DS/PSS/AA)

(CT:ORG-149; 02-16-2006)

- a. Serves as single point of contact for the Bureau of Diplomatic Security for all requests for investigative records checks, i.e., promotion, tenure, D Committee, etc., to the HR.
- b. Serves on ad-hoc (Personnel Security Working Group) interagency working groups to address personnel security issues throughout government.
- c. Determines the suspension, revocation or subsequent reinstatement of security clearances for personnel, under the cognizance of DS/SI/PSS, as well as performing adjudicative determinations recommending assignment restrictions for Department personnel.

1 FAM 266.3-4 Customer Service Division(DS/PSS/CS)

(CT:ORG-149; 02-16-2006)

- a. Assists Department personnel and HR Specialists in every aspect of the security clearance process, to include the performance of training requirements.
- b. Reviews initial security clearance request documentation for consideration of an interim security clearance, upon request. Adjudicates, as appropriate, and responsible for interim access suspension/withdrawal.
- c. Manages and maintains the personnel security records program.
- d. Verifies and certifies security clearances on all applicants under reciprocity standards.
- e. Processes frequent visitors to and from Department facilities and other agencies.
- f. Administers the Contract Review Panel and security/suitability

determinations for contract applicants/employees to the Department. Processes and has final determination authority for all reconsideration requests.

- g. Coordinates all case referrals to the Civil Service Personnel Review Panel and provides DS representation to the panel. Works with Panel Chairperson in establishing case agenda.
- h. Co-responsible with other areas of PSS for final draft, review and completion of Presidential-appointee summary packages.

1 FAM 267 THROUGH 269 UNASSIGNED

1 FAM EXHIBIT 261.2

BUREAU OF DIPLOMATIC SECURITY (DS)

(CT:ORG-160; 07-06-2006)

